Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Хуторного Олександра Сергійовича*

академічної групи *125-22м-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Методи виявлення та протидії фішингу в соціальних мережах та месенджерах*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Котух.Є.В.			
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц., Пілова Д.П.	95	Відмінно	
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту *Хуторному Олександру Сергійовичу* **академічної групи** *125-22м-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Методи виявлення та протидії фішингу в соціальних мережах та месенджерах***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 09.10.23 № 1227-С

Розділ	Зміст	Термін виконання
Розділ 1	Визначити актуальність питання та провести аналіз об'єкту дослідження. Розкрити поняття фішингу, його мету, види та підвиди фішингових атак. Проаналізувати статистику, навести стандартні рекомендація.	05.11.2023
Розділ 2	Визначити роль соціальної інженерії у фішингових атаках, створити тестовий стенд фішингового сайта для демонстрації фішингу. Навести приклад фішингу на маркетплейсах і благодійних платформах. Розробити рекомендації до наведених моделей фішингу.	20.11.2023
Розділ 3	Обґрунтувати доцільність використання наведених методів, підрахувати витрати на впровадження рекомендацій та їх поширення, розрахувати коефіцієнт повернення інвестицій.	01.12.2023

Завдання видано _____ Євген КОТУХ
(підпис керівника) (ім'я, прізвище)

Дата видачі: 01.09.2023

Дата подання до екзаменаційної комісії: 08.12.2023

Прийнято до виконання _____ Олександр ХУТОРНИЙ
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 86 с., 38 рис., 2 табл., 4 додатка, 20 джерел.

Об’єкт дослідження: інтернет шахрайства, фішинг, соціальна інженерія.

Мета кваліфікаційної роботи: дослідити сучасні методи фішингу, вплив шахраїв на жертву за допомогою соціальної інженерії та розробити універсальні рекомендації для підвищення рівня обізнаності користувачів у сфері захисту особистої інформації.

У кваліфікаційній роботі розглядається проблематика та актуальність кібербезпеки на сьогодення. Визначено актуальність питання підвищення рівня знань користувачів у соціальних мережах та месенджерах з наведенням статистики збитків від фішингу. Визначено мету фішингових атак, їх види, механізм з урахування соціальної інженерії. Проведено моделювання фішингових атак та представлені стандартні рекомендації, щодо захисту від фішингу.

Розкрито поведінку порушника, його тактику та основні прийоми під час активної фази фішингу, розглянуто сучасні моделі фішингу та їх реалізацію на стенді зі створенням фішингового сайта з отриманням даних від користувачів, створено універсальну пам’ятку для користувачів про безпеку в інтернеті для певних платформ розповсюждення.

У економічному розділі підрахували доцільність розповсюдження пам’яток та банерів про безпеку під час користування інтернет ресурсами з метою підвищення рівня знань користувачів про кібербезпеку та фішинг. Розраховані капітальні витрати на створення та утримання проекту та коефіцієнт повернення інвестицій, який показав доцільність впровадження проекту для збереження коштів держави і громадян.

Практичне значення роботи полягає у підвищенні знань про шахрайство в інтернеті з метою зменшення кількості кіберзлочинів.

ІНФОРМАЦІЙНА БЕЗПЕКА, СОЦІАЛЬНІ МЕРЕЖІ, ФІШИНГ, ШАХРАЙСТВО, КІБЕРБЕЗПЕКА, СОЦІАЛЬНА ІНЖЕНЕРІЯ.

ABSTRACT

Explanatory Note: 86 Pages, 38 Pictures, 2 Tables, 4 Appendices, 6 Sources.

Research Object: internet fraud, phishing, social engineering.

Objective of the qualification work: To investigate modern phishing methods, the impact of scammers on the victim through social engineering, and to develop universal recommendations to enhance users' awareness in the protection of personal information.

The qualification work addresses the issues and relevance of cybersecurity today. The significance of raising users' knowledge in social networks and messengers is identified, accompanied by statistics on losses from phishing. The purpose of phishing attacks, their types, and the mechanism involving social engineering are defined. Modeling of phishing attacks is conducted, and standard recommendations for protection against phishing are presented.

The behavior of the offender, tactics, and main techniques during the active phase of phishing are disclosed. Modern phishing models and their implementation on a platform with the creation of a phishing site for obtaining user data are discussed. A universal safety guide for internet use on specific distribution platforms is created.

In the economic section, the feasibility of distributing safety guides and banners during internet resource usage is calculated to increase user knowledge about cybersecurity and phishing. Capital expenditures for project creation and maintenance, as well as the return on investment coefficient, demonstrate the feasibility of implementing the project to save state and citizen funds.

The practical significance of the work lies in increasing knowledge about internet fraud to reduce the number of cybercrimes.

INFORMATION SECURITY, SOCIAL NETWORKS, PHISHING, FRAUD, CYBERSECURITY, SOCIAL ENGINEERING.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

БПЗ – бот прийому заявок;

КГ – крипто гаманець;

КС – комп’ютерна система;

МП – мобільний пристрій;

МРС– массована розсилка спаму;

ОС – операційна система;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ПФО – підробна форма оплати;

РП – рекламний пост;

ФП – фішингове посилання.

ЗМІСТ

ВСТУП

У часи активного розвитку кіберзлочинності, зростає кількість кіберзлочинів та випадків інтернет шахрайств. Найбільш необізнаним сектором користувачів мережі інтернет є приватні особи, які становлять більшість серед зареєстрованих випадків з кіберполіції.

Комп'ютерне шахрайство (кібершахрайство) – це введення, заміна, виправлення, знищення комп'ютерних даних або програм чи інші втручання до процесу обробки інформації, які впливають на кінцевий результат, спричиняють економічні або майнові збитки з метою одержання незаконного економічного прибутку для себе чи іншої особи.[1]

Для вирішення цих питань необхідно підвищити обізнаність користувачів соціальних мереж, месенджерів, та інших платформ з питань безпеки поводження та поширення інформації в інтернеті. Для цього необхідно створити рекомендації як не потрапити до пастки шахраїв та поширити її в маси.

Для розробки рекомендацій для користувачів необхідно вивчити нові методи шахрайств, зокрема фішингові як найбільш популярні, ознайомитися з принципом їх роботи та навчитися розпізнавати фішингові посилання.

Фішинг – вид шахрайства, метою якого є виманювання в довірливих або неуважних користувачів мережі персональних даних клієнтів онлайн аукціонів, сервісів із переказу або обміну валюти, інтернет–магазинів. Шахраї намагаються змусити користувачів самостійно розкрити конфіденційні дані – наприклад, надсилаючи електронні листи з пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на сайт, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів.[2]

Тільки розглянувши сучасні методи фішингу від початку створення ідеї, до отримання прибутку та методів їх отримання, зможемо оглянути процес створення кібершахрайських схем.

Об’єкт розробки: рекомендації для підвищення рівня знань користувачів про захист персональних даних та кібершахрайство в інтернеті.

Предмет дослідження: фішинг в соціальних мережах і месенджерах, модель поведінки шахрая та вплив соціальної інженерії на жертв.

Мета розробки: дослідити сучасні методи фішингу, вплив шахраїв на жертву за допомогою методів соціальної інженерії та розробити універсальні рекомендації для підвищення рівня обізнаності користувачів у сфері захисту особистої інформації.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Актуальність питання

Кожного дня у світі люди переписуються зі своїми друзями, дивляться новини та фото своїх близьких або знайомих, купують та продають речі, їжу, техніку, тощо. Більшість з них роблять це через смартфон, дехто з персонального комп'ютера, та з інших пристроїв, але всі ці люди об'єднані між собою глобальною мережею інтернет. Мало хто з них замислюється що кожні 39 секунд у світі відбувається кібератака, у порівнянні з 2022 роком кількість фішингових сайтів збільшилася на 61%, кожні 10 секунд хтось відкриває файл-вимагач.

Статистика не може надати читках даних, у зв'язку з тим, що не кожна жертва говорить про це відкрито, або фіксує такі випадки за допомогою подачі заяв у відповідні органи влади.

Кожного року кількість кіберзлочинів збільшується, зловмисникам легше знаходити нові схеми для виманювання коштів, їх можливості та варіації впливу на жертву зростають кожен день. Про захист у певних видах шахрайства як у старій приказці: "Спасіння потопаючого – у руках потопаючого". Щоб не стати жертвою шахраїв необхідно самостійно вивчити як діють шахраї щоб вміти розпізнати випадки обману в інтернеті.

На більшості сайтів та платформ є правила поводження на ресурсах, їх політики безпеки, застереження для користувачів, але більшість людей їх просто ігнорує, недотримується або взагалі не знає про них.

Спираючись на данні Національного Банка України за 2022 рік, які показані на рис. 1.1, сума збитків від шахрайських дій пов'язаних з банківськими картками збільшилась, при цьому відсоток дій через торгівельні мережі та банкомати зменшився, а от через мережу інтернет збільшився.

Рисунок 1.1 – Збитки від незаконних дій із платіжними картками

Згідно росту всіх показників можна зробити висновки про рівень кібершахрайства в Україні. З кожним роком про цю проблему дізнаються все більша кількість громадян, але навіть ті хто знає про кібершахрaство, як оманюють на більшості серсівах, все одно стають жертвами шахраїв і зовсім не через уважність, а саме через невміння розпізнавати шахрайські дії.

На сьогоднішній день кібершахрайство стало зручним методом для шахраїв, оскільки у кіберпросторі вони можуть максимально безпечно виманювати кошти у жертви, використовуючи фейкові номери телефонів, нові аккаунти без прив’язок до документів, виходячі в інтернет через проксі-сервери бути у безпеці.

Насамперед необхідно підвищити обізнаність людей у сфері кіберзахисту та кібершахрайтсва, щоб зменшити кількість злочинів, зменшити навантаження на органи правопорядку та підвищити показники захищеності кіберпростору країни.

Згідно даних отриманих від банків, можна зробити висновок, що кожного року кількість шахрайств збільшується, кількість збитків державі та страховим компаніям збільшується, а це означає, що кількість робочих місць з питань безпеки у виробничому та соціальному секторі збільшує свою актуальність, як можна це помітити на рис. 1.2.

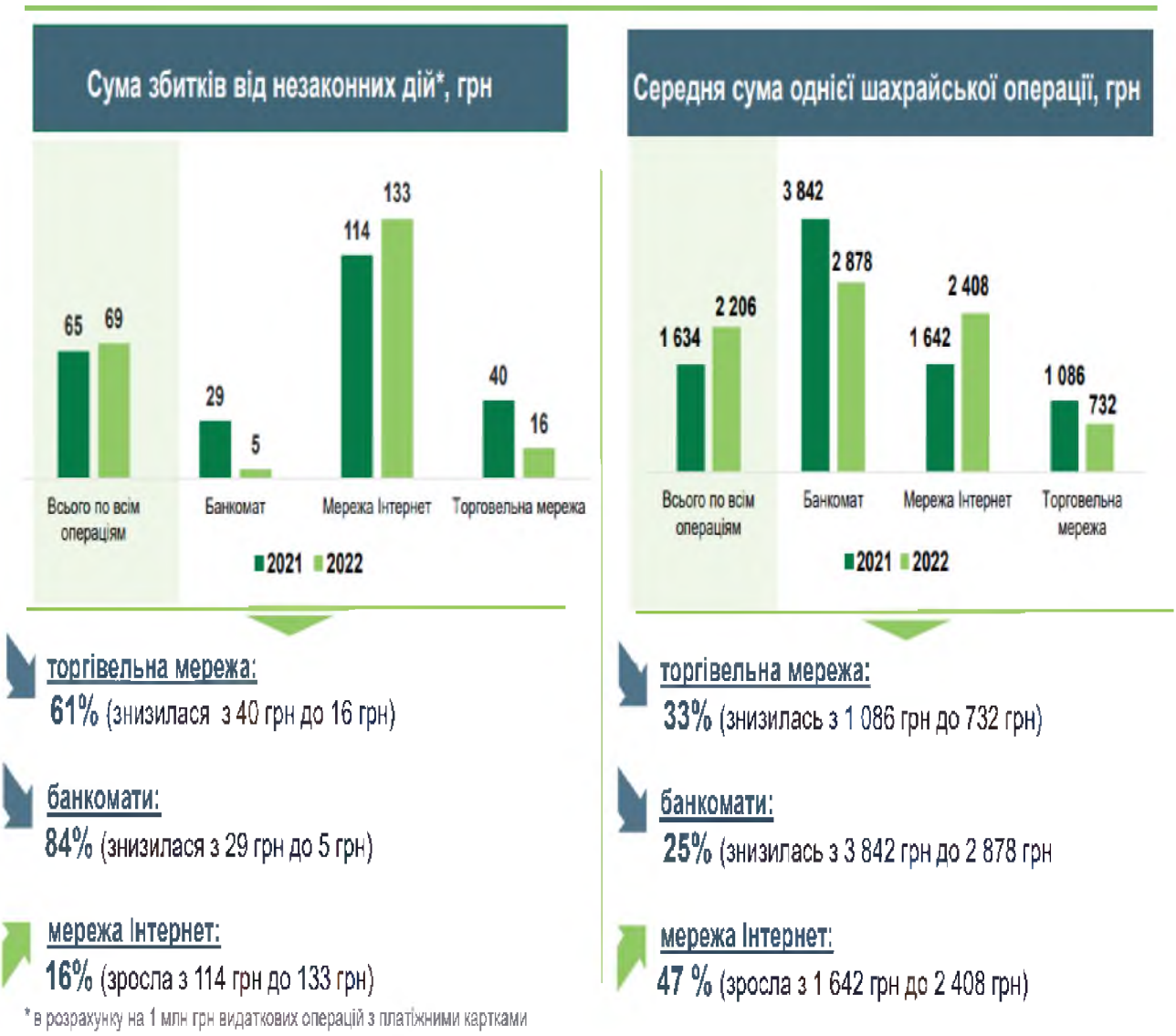

Рисунок 1.2 – Збитки від незаконних дій із платіжними картками за каналами здійснення операцій

При збільшенні попиту на захист інформації, прийняття заяв від громадян, розслідування інцидентів інформаційної безпеки, потребує виділення коштів у

види заробітної платні персоналу, компенсації збитків, зростає і завдає збитків не тільки громадянам, а і фінансовому та державному сектору.

1.2 Аналіз об'єкту дослідження

Фішинг – один із простих, легких у реалізації та прибутковий методів, який не вимагає знань у програмуванні, особливих складних інструментів, не вимагає великих фінансових вкладень та простий у реалізації, більшість схем у вільному доступі в інтернеті.

Фішинг став одним із най поширеним методом кіберзлочинів в Україні за останні три роки, використовується на всіх платформах оголошень, месенджерах, соціальних мережах, у сборі коштів для військових, тощо.

1.2.1 Мета фішингу

Фішинг існує впродовж багатьох років, за цей час кіберзлочинці розробили широкий спектр методів інфікування жертв.

Найчастіше зловмисники, які займаються фішингом видають себе за банки чи інші фінансові установи, щоб змусити жертву заповнити фальшиву форму та отримати дані облікових записів.

У минулому для виманювання даних користувачів кіберзлочинці часто використовували неправильно написані або оманливі доменні імена. Сьогодні зловмисники використовують більш складні методи, завдяки чому фальшиві сторінки дуже схожі на свої легітимні аналоги.

Викрадені дані жертв, зазвичай, використовуються для викрадення коштів з банківських рахунків або продаються в Інтернеті. Подібні атаки здійснюються також через телефонні дзвінки (vishing) та SMS-повідомлення (smishing).

Серед методів виманювання коштів в інтернеті можуть зустрічатися шахрайства пов'язані з покупками, з продажем та розрахунками банківськими картками, віруси-шифрувальники та шкідливе ПО, інтернет жебрацтво, афери та лотереї, неіснуючі магазини, пропозиції вирішення проблем, закриття боргів, заробітку, тощо (рис. 1.3).

Рисунок 1.3 – Методи виманювання коштів через інтернет

Цілеспрямований фішинг – кіберзлочинці, які використовують цей метод, зазвичай, заздалегідь детально досліджують свою ціль. Це значно ускладнює ідентифікацію вмісту як шкідливого.

Як розпізнати фішинг? Електронне повідомлення може містити офіційні логотипи або інші ознаки авторитетної організації. Нижче наведено кілька підказок, які допоможуть виявити фішингове повідомлення.

– Загальні або неофіційні привітання – листи без персоналізації (наприклад, «Шановний клієнт») та формальностей, має викликати підозри. Те ж саме відноситься до псевдо-персоналізації з використанням випадкових, підроблених посилань.

– Запит на особисту інформацію – часто використовують кіберзлочинці, але банки, фінансові установи та більшість онлайн-сервісів намагаються цього уникати.

– Некоректна граматика – орфографічні та друкарські помилки, а також незвичайні фрази часто можуть означати небезпеку (але відсутність помилок не є доказом легітимності).

– Несподівані повідомлення – будь-який незапланований контакт з банком повинен викликати підозри.

– Терміновість – фішингові повідомлення часто намагаються викликати відчуття терміновості дій, залишаючи жертвам менше часу на роздуми.

– Пропозиція, від якої важко відмовитися – якщо лист занадто хороший, щоб бути правдою, він, напевно, є фішинговим.

– Підозрілий домен – чи дійсно американський чи німецький банк надсилатиме електронний лист з китайського домену?

Як захиститися від фішингу? Щоб уникнути подібних атак, звертайте увагу на описані вище ознаки, за допомогою яких можна виявити фішингові повідомлення.

– Дізнавайтесь про нові методи фішингу: читайте засоби масової інформації для отримання нової інформації про фішингові атаки, оскільки кіберзлочинці постійно знаходять нові методи для виманювання даних користувачів.

– Не надсилайте облікові дані: будьте особливо уважні, коли у електронному листі начебто перевірені організації запитують ваші облікові або інші конфіденційні дані. У разі необхідності перевірте вміст повідомлення, відправника або організацію, яку вони представляють.

– Не натискайте на підозрілі кнопки та посилання: якщо підозріле повідомлення містить посилання або вкладення, не натискайте та не завантажуйте вміст. Це може призвести до переходу на шкідливий веб-сайт або інфікувати ваш пристрій.

– Регулярно перевіряйте облікові записи: навіть якщо ви не маєте підозр, що хтось намагається викрасти ваші облікові дані, перевірте банківські та інші облікові записи в Інтернеті на наявність підозрілої активності.

1.2.2 Еволюція від початкових стадій інтернет-омани до сучасних витончених методів

Початковий період: на зорі епохи інтернету, фішингові атаки були простими та здебільшого спрямовані на користувачів комп'ютерних мереж, таких як AOL (American Online). Зловмисники надсилали листи, вимагаючи підтвердити паролі або платіжні дані.

Середина 2000-х: з появою електронної комерції та банківських послуг онлайн фішинг став більш розповсюдженим. Сайти банків і платіжних систем стали основними цілями для атак.

Сучасність: з розвитком технологій, фішингові атаки стали набагато витонченішими. Щоб обійти захист, зловмисники використовують SSL-шифрування, змішують URL, створюють фейкові вебсайти, які майже ідентичні оригіналам.

Коротка хронологія значущих фішингових інцидентів:

2003 рік: Була запущена атака на клієнтів E-Gold, однієї з перших електронних платіжних систем.

2004 рік: Користувачі eBay стали жертвами однієї з найбільших фішингових кампаній, де зловмисники намагалися вкрасти особисті дані та паролі.

2007 рік: Зловмисники використали атаку на клієнтів Bank of America, вимагаючи підтвердити свої банківські дані через специфічні посилання.

2009 рік: Популярний соціальний мережевий ресурс LinkedIn було атаковано фішинговою кампанією, що цілилась у користувачів, намагаючись викрасти їх облікові дані.

2011 рік: RSA Security, компанія з кібербезпеки, визнала, що стала жертвою витонченої фішингової атаки, яка призвела до витоку інформації про їх систему двофакторної автентифікації.

2013 рік: Одна з найбільших атак на клієнтів Apple ID, де користувачам надсилалося повідомлення про необхідність підтвердити свої дані.

2014 рік: Користувачі Google стали мішенями обширної фішингової атаки, яка стверджувала, що їхні аккаунти були скомпрометовані.

2016 рік: Yahoo! повідомила про масову фішингову атаку, спрямовану на мільйони її користувачів.

2017 рік: Найбільший фішинговий інцидент був спрямований проти користувачів Gmail, де зловмисники створили вигляд, ніби додаток Google Docs намагається отримати доступ до користувацьких аккаунтів.

Ці приклади демонструють, наскільки широким і постійно змінюваним є феномен фішингу, який впливає на користувачів Інтернету у всьому світі.

1.2.3 Види та підвиди фішингових атак

Spear phishing (Спеціалізований фішинг).

Опис: Ця форма фішингу цілеспрямовано атакує конкретних осіб або організацію.

Схема роботи: Шахраї збирають інформацію про свою ціль, таку як інтереси, зв'язки, робочі обов'язки тощо. Вони потім створюють персоніфіковані електронні листи, які можуть виглядати, як від відомої для жертви особи чи організації, намагаючись спонукати їх надати конфіденційні дані або клікнути по шкідливому посиланню.

Vishing (Вішинг).

Опис: Це фішинг за допомогою голосового зв'язку.

Схема роботи: Зловмисники телефонують жертві, виступаючи в ролі банку, служби підтримки або іншої офіційної організації. Вони можуть стверджувати, що є проблеми з рахунком жертви, вимагають перевірки особистої інформації або інших даних, намагаючись отримати конфіденційну інформацію від жертви.

Smishing (Смішинг).

Опис: Шахраї використовують SMS-повідомлення для обману.

Схема роботи: Жертва отримує текстове повідомлення, яке містить посилання на шкідливий сайт, пропозицію завантажити додаток або інструкції про відправку текстового повідомлення на певний номер. Посилання може призвести до встановлення шкідливого ПЗ на пристрій жертви або до фішингового сайту, який вимагає введення особистих даних.

Pharming (Фармінг).

Опис: Цей метод полягає у перенаправленні користувачів зі справжнього сайту на підробний.

Схема роботи: Зловмисники атакують DNS-сервери або файл hosts на комп'ютері жертви, щоб перенаправити запити до певного домену на інший, шкідливий, сервер.

Whaling (Вейлінг).

Опис: Це тип spear phishing, спрямований на високопоставлених осіб в організації, таких як виконавчі директори.

Схема роботи: Атаки вейлінга зазвичай більш витончені, використовуючи персоналізовані повідомлення адресовані на певних вже відомих персон для атаки, які можуть включати корпоративну термінологію. Мета – отримати доступ до фінансової інформації або інших цінних ресурсів організації.

Clone phishing (фішинг клонування).

Опис: Це метод, при якому легітимний, раніше доставлений, електронний лист клонується і змінюється, щоб включити шкідливе посилання або вкладення.

Схема роботи: Зловмисники беруть реальний електронний лист, який був раніше відправлений постачальником послуг, та замінюють легітимне вкладення чи посилання на шкідливий варіант, потім відправляють цей "оновлений" лист від імені відомого відправника.

1.2.4 Механізми фішингових атак: психологічні принципи та технічні аспекти

Зловмисники часто використовують основні психологічні принципи для маніпулювання своїми жертвами. Серед них:

– Терміновість: Шахраї створюють ілюзію необхідності терміново вжити дій, щоб викликати поспіх і паніку у жертви.

– Страх: Зловмисники можуть намагатися налякати людей, стверджуючи, що їхній банківський рахунок або особисті дані можуть бути викрадені.

– Знайомість: Шахраї намагаються виглядати як легітимні організації або відомі особи, використовуючи логотипи, стиль спілкування та інші відомі деталі.

Технічний розбір фішингових атак.

Фішингові атаки є однією з найпоширеніших форм кіберзлочину. На комп'ютерному рівні вони базуються на декількох ключових компонентах, які детально описані нижче:

Підроблені вебсайти / фішингові сайти:

Як це робиться: Зловмисники створюють вебсайти, які візуально майже ідентичні легітимним сайтам, як-от банківські сайти, соціальні мережі чи служби електронної пошти. Це може бути здійснено за допомогою спеціалізованих інструментів або просто копіюючи код та дизайн оригінального сайту.

Для чого: Ціль таких сайтів – змусити користувача ввести свої особисті дані, такі як логін та пароль, номер кредитної картки чи іншу конфіденційну інформацію.

Шкідливі посилання:

Як це робиться: Зловмисники розсилають посилання на підроблені сайти або шкідливий контент через електронні листи, повідомлення в соцмережах, SMS або інші засоби комунікації.

Для чого: Мета – змусити жертву клікнути на посилання і, можливо, ввести свої персональні дані на шахрайському сайті або завантажити шкідливий файл.

Вірусне ПЗ:

Як це робиться: Якщо користувач клікає по шкідливому посиланню або завантажує підозрілі вкладення, на його комп'ютер може бути завантажено вірусне ПЗ. Це може бути троян, шпигунське ПЗ або інші типи шкідливих програм.

Для чого: Ці програми можуть використовуватися для збору особистої інформації, злому аккаунтів, шпигунства або включення комп'ютера жертви до мережі заражених комп'ютерів (ботнету – мережі комп'ютерів зомбі).

1.2.5 Реальний приклад фішингу

Одним з найбільш популярних прикладів фішингу в Україні є атаки, пов’язані з платформою оголошень “OLX”.

Зловмисники використовують тактику, засновану на фальшивій службі “OLX Доставка”. Схема дій така, як показона на рис 1.4:

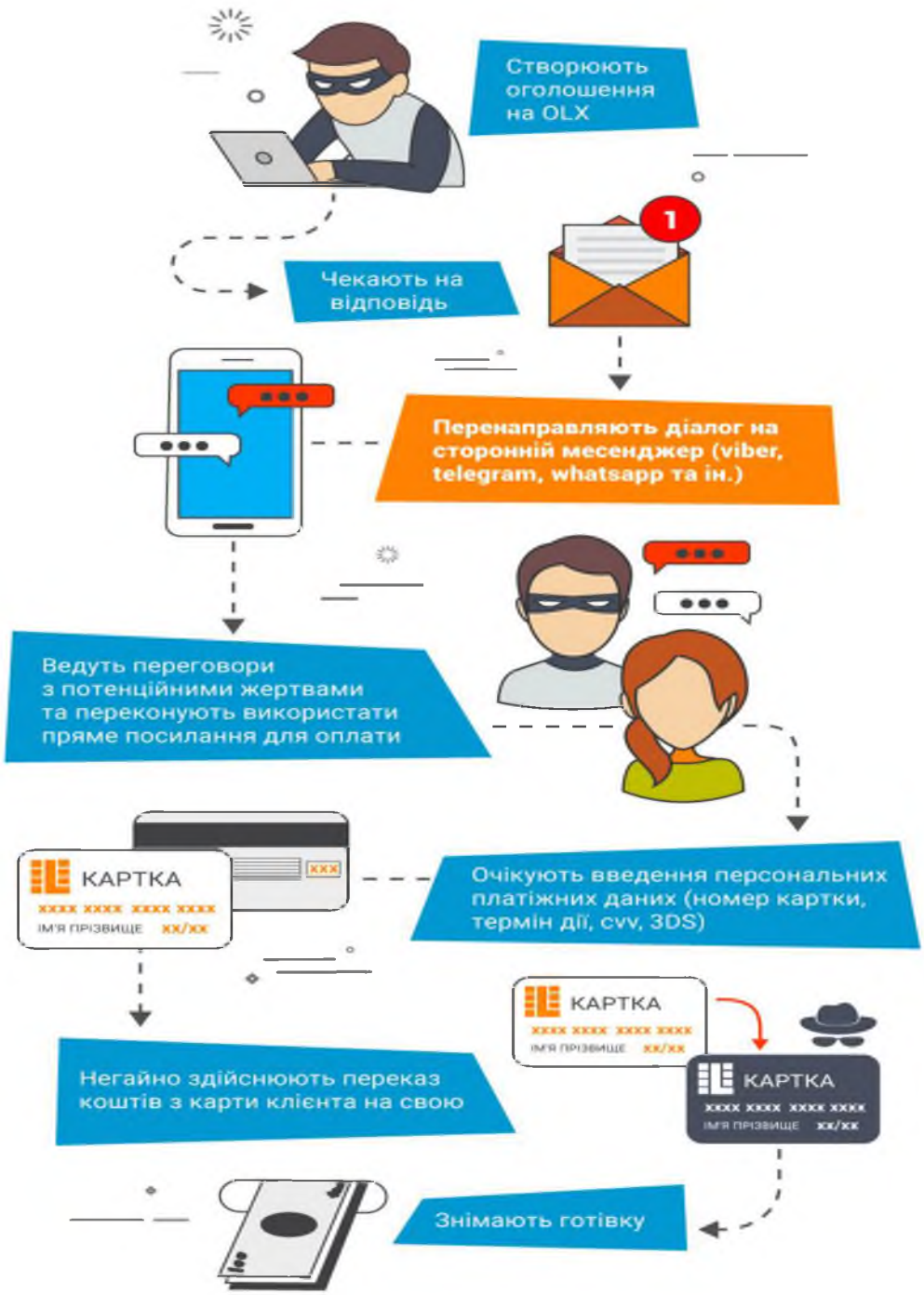

Рисунок 1.4 – Схема дій зловмисника на прикладі сервісу “OLX”

Створення оголошення: Шахраї розміщують привабливі оголошення про продаж товарів за цінами, що часто є нижчими від ринкової вартості, щоб привернути увагу покупців.

Перший контакт: Коли потенційний покупець зв'язується зі шахраєм, останній пропонує використовувати "OLX Доставку" для безпечної угоди.

Фальшива служба доставки: Шахраї відправляють фальшиві документи або посилання на сайти, які імітують реальний OLX, де покупцеві пропонуються деталі для оплати товару.

Оплата: Покупець, вважаючи, що угода безпечна, здійснює оплату на рахунок шахрая.

Відсутність товару: Після отримання грошей, зловмисник перестає відповідати на дзвінки та повідомлення, а товар, звісно, не відправляється.

Ця тактика використовує довіру користувачів до відомої та надійної платформи OLX. Внаслідок цього, багато людей стають жертвами цих атак, не перевіряючи достовірність інформації, яку вони отримують. OLX активно бореться з такими шахраями, регулярно надаючи рекомендації своїм користувачам як розпізнавати та уникати фішингових атак.

Покрокова схема фішингу може виглядати так:

– Зловмисник створює оголошення на платформах з продажу товару, при цьому зазвичай вказує низьку ціну, ідеальний стан або інші аспекти товару, щоб зацікавити як найбільше покупців.

– Під час переписки з жертвою може маніпулювати, пришвидшувати рішення купівлі, пропонує зв'язатися в інших місцях, наприклад месенджерах "вайбер" або "телеграм".

– Після переконання придбати товар, зловмиснику необхідно дізнатися інформацію з банківських карток, він може запитувати, просити фото картки або використовувати сторінку фейкової оплати.

– Після отримання даних карток, зловмисники роблять купівлю криптовалюти, речей чи послуг або виводять гроші на інші картки.

На сьогоднішній день метод здобуття особистого прибутку від фішингу є дуже різноманітнім, оскільки він може пересікатися з іншими нелегальними схемами відмивання грошей. Наприклад вже давно існує метод збуту товарів, куплених з крадених карток з використанням купівлі з інших країн. Якщо картку банку було викрадено в Україні, можна активувати купівлю онлайн з більшим лімітом, придбати новий телефон в Німеччині, де третя особа його отримає та перепродасть при цьому отримуючи гроші, згодом пересилаючи зловмиснику його долю.

За останні роки шахрайство в Україні зростає через зменшення робочих місць у зв'язку з корона вірусом та повномасштабною війною. Велика навантаженість на співробітників Міністерства Внутрішніх Справ України, Служби Безпеки України зменшили сроки розгляду справ, а кількість проваджень тільки збільшилася. Це означає що час, необхідний для розкриття злочинності, або час реагування збільшується. Згідно статистики останніх років більшість жертв не звертаються до правоохоронних органів, хоча раніше звертався кожен другий. Всі ці фактори збільшили кількість шахраїв в інтернеті, які відчувають безкарність, легкість реалізації фішингу, оскільки схеми з інструкціями є у вільному доступі в інтернеті.

За результатами опитування користувачів OLX за 2022 рік серед 75 тисяч опитуваних, було виявлено наступні данні.

– Основними цілями фішингу обирають в більшій ступені жінок 65%, ніж чоловіків 35%.

– Кількість жертв, що звертаються до правоохоронних органів зменшилася з 21% до 10% в порівнянні з даними за 2020 рік.

– Серед опитуваних 50% зіштовхувалися з фітингом, а 14% втратили власні кошти через фітинг.

– Жителі великих міст стають жертвами шахрайства частіше ніж мешканці невеликих міст та селищ.

– Приблизно 54% шахрайств є продажем неіснуючого товара, 28% використання підробних форм оплати, 11% надсилання фальшивих скріншотів оплати.

– 83% фішингових атак відбувається у сторонніх месенджерах, наприклад Телеграм, Вайбер.

– 6% атак відбувається черес СМС фітинг.

– 2% атак відбувається за допомогою пошти.

1.3 Статистика кібершахрайства в Україні.

Щоб визначити глобальність проблеми в Україні, необхідно провести дослідження, в порівнянні декількох років та різних груп населення. Згідно даним Кіберполіції тенденція кібершахрайств зростає, як наведено у табл. 1.1, при цьому люди більше почали самостійно вирішувати свої проблеми, не звертаючись до працівників Кіберполіції.

Таблиця 1.1 – Статистика реагування на шахрайські дії

Що ви робите, якщо стикаєтесь із шахрайством в інтернеті? (оберіть декілька варіантів)	2021 рік	2022 рік
Намагаюся розв’язувати свої питання самостійно	35%	51%
Розповідаю близьким	56%	41%
Звертаюся до Служби підтримки онлайн-ресурсу	39%	13%
Звертаюся до Кіберполіції	23%	10%
Не роблю нічого	18%	25%
Звертаюся за допомогою до знайомих	8%	15%

З статистики серед громадських опитувань приблизно 18% не знають що робити з шахрайством в інтернеті та не знають як йому протидіяти. За рік близько 16% всього населення України отримували фішингові посилання від шахраїв. А

про методи протидії шахрайству 51% опитаних в цьому році вже дізналися з соцмереж, 31% від друзів, 18% з телебачення. Майже 40% українців уже знають, що надіслані посилання від малознайомих людей можуть бути шахрайською атакою, тому не відкривають їх і не обговорюють фінансові питання в месенджерах, якщо співрозмовник поводиться підозріло. 20% перевіряє користувача за номером телефону, 14% уважно вчитується в зміст сторонніх SMS та поштових листів, а 10% перевіряє посилання сайтів, щоб не потрапити на шахрайський сайт-копію.

Багато методів використовують для шахраювання над українцями в інтернеті: пенсіонерів ошукують, наприклад, утричі частіше за інших – через SMS про виграш у лотерею, кожного четвертого підлітка після відкриття фішингового посилання. Мешканці сіл частіше натрапляють на продаж неіснуючого товару по передоплаті, а кияни – на фішингові атаки. Стать, до речі, практично не впливає на вірогідність зустріти шахрая в інтернеті. Місце проживання значно впливає на тип шахрайств. Наприклад, дві треті жителів селищ міського типу та сіл стикаються зі спробами продати їм неіснуючий товар за передоплатою, а от жителі міст у 1,5 раза частіше отримують фішингові посилання. Жителі райцентрів на третину частіше за інших стикаються з підробленими квитанціями про оплату. У селах в цілому менше обізнаних з базовими правилами кібербезпеки. Якщо понад 42% містян не ведуть спілкування за межами платформи, де здійснюють угоду, та не відкривають посилання від незнайомих людей, то серед мешканців сіл, це тільки 33% опитаних. Водночас жителі столиці найбільше потерпають від фішингу, а от у Дніпрі, Одесі, Харкові та Львові половина випадків пов’язана з передоплатою неіснуючого товару. Найбільш відповідально до звернень у Кіберполіцію ставляться у Львівській області, кожний 8-ий ошуканий подасть заяву, а найменш в Одеській тут звернеться тільки кожний 14-ий. Серед всіх вікових категорій 80% випадків онлайн-шахрайств відбуваються у месенджерах. Пенсіонерам утричі частіше надсилають шахрайські SMS, у сім раз електронні листи про “виграш в лотерею”, “нові умови тарифу” чи “правила карантину”. Водночас 57% українців віком від 46 до 65 років натрапили

на шахраїв, які просили зробити передоплату за неіснуючий товар. Молодь віком 18 до 25 років у кожному третьому випадку натрапляє на фітинг, як це наведено у табл.1.2, а кожний четвертий неповнолітній втратив гроші після переходу за шкідливим посиланням на сайт підробку відомого бренду. Це пов'язано з тим, що молодь більше за старше покоління проводить час в онлайні, але так само слабо обізнана з базовими правилами кібербезпеки. Молодь більш обізнана з базовими правилами кібербезпеки, однак загальний рівень навичок онлайн-поведінки лишається невисоким.[3]

Таблиця 1.2 – Статистика поведінки в інтернеті за віком

Правила кібербезпеки	до 18 років	Від 18 до 65 років	після 65 років
Не відкривають посилання від незнайомців	48%	51%	28%
Не розголошують платіжні дані банківської картки	30%	42%	29%
Звертають увагу на оцінки і відгуки	38%	35%	19%
Не обговорюють угоду поза платформою	39%	40%	38%
Перевіряють номер продавця/покупця в базах відгуків	26%	28%	21%
Уважно оцінюють текст в SMS чи пошті	22%	19%	14%
Звертають увагу на манеру спілкування	45%	42%	38%

Використовуючи знання, отримані з статистики, можна зробити висновки, щодо кібершахрайств в Україні за останні роки. Збільшилася тенденція фішингу, вішингу та інших видів інтернет-шахрайств, зменьшилася довіра до Кіберполіції та страхових структур. Ця тенденція збільшується кожного року, оскільки персональні навички населення з приводу захисту себе та своїх персональних даних в інтернеті не підвищується, а навіть падає до рівня початкових

користувачів. Оскільки кожного дня користувачів інтернету стає дедалі більше, а рівень освідченності користуванням інтернету не підвищується, жертви шахраїв нажаль навчаються на своїх помилках, інколи не на одній помилці.

1.4 Рекомендації щодо захисту від фішерів

Люди всіх вікових категорій стають мішенями для фішерів. Деякі літні особи можуть отримувати сповіщення, які намагаються імітувати повідомлення від офіційних установ або банків, тоді як студенти можуть отримувати інформацію про “стипендії”, які вони нібито “виграли”. Але, щоб уникнути підстав, на які спирається фішинг, ось 10 конкретних порад, які допоможуть захистити вас від цих підступних атак:

- Подвійна перевірка посилань: Перед тим, як клікнути по посиланню в електронному листі, наведіть на нього курсор, щоб перевірити, куди веде це посилання. Якщо вебадреса виглядає підозріло, не клікайте.
- Будьте обережними з вкладеннями: Ніколи не відкривайте вкладення від незнайомців. Це може бути вірус або шкідливе ПЗ.
- Використовуйте двофакторну аутентифікацію: Ця додаткова міра безпеки вимагає підтвердження входу через додатковий пристрій або додаток.
- Оновлюйте своє ПЗ: Регулярно оновлюйте своє програмне забезпечення, щоб уникнути вразливостей.
- Не відповідайте на підозрілі повідомлення: Якщо лист виглядає підозріло, навіть якщо він нібито від відомої вам особи або компанії, краще зв’язатися з цією особою або компанією безпосередньо.
- Використовуйте антивірус: Регулярно перевіряйте свої пристрої на наявність вірусів та шкідливого ПЗ.
- Будьте критично налаштованими: Якщо щось здається занадто гарним, щоб бути правдою, ймовірно, це так і є.
- Перевіряйте джерела інформації: Не слідуйте інструкціям з електронних листів без перевірки, чи дійсно вони від надійного джерела.

– Використовуйте захищені підключення: Завжди переконуйтеся, що використовуєте захищене підключення (https), особливо коли вводите особисту або фінансову інформацію.

– Освіта та навчання: Регулярно оновлюйте свої знання з кібербезпеки. Знання – це ваш найкращий захист.

Дотримуючись цих порад, ви значно знизите ризик стати жертвою фішингових атак у своєму щоденному житті.

Фішинг у соціальних мережах: небезпека перевантаження інформацією.

Соціальні мережі – це місце, де люди часто діляться особистою інформацією, і це може бути використано шахраями. Тактика соціальної інженерії дозволяє зловмисникам з'ясовувати особисту інформацію жертви, використовуючи її потім для фішингових атак. Наприклад, поширеним є використання інформації про друзів, родину або події з життя людини, зібраної з її профілю у соцмережі, для створення переконливих повідомлень або електронних листів.

Виявлення спроби фішингу: як розпізнати загрозу?

Кожного дня ми отримуємо безліч повідомлень і сповіщень на своїх електронних адресах та мобільних пристроях. Але як розпізнати, яке з них є спробою обману?

Ознаки типового фішингового повідомлення:

– Незвичайна адреса відправника: Якщо ви отримали лист від організації, з якою спілкуєтеся, але адреса відправника виглядає підозріло, це може бути спробою фішингу.

– Помилки в тексті: Шахрайські листи часто містять орфографічні та граматичні помилки.

– Спроби викликати паніку: Шахраї намагаються спровокувати вас на швидкі дії, заявляючи про проблеми з вашим рахунком або втрату доступу.

– Посилання на підозрілі сайти: Замість клікання на такі посилання, варто набрати адресу сайту вручну в браузері.

Як відрізнити справжнє повідомлення від шахрайського? Завжди перевіряйте звідки приходить лист. Якщо у вас виникли сумніви, зателефонуйте в організацію напряму (не використовуючи контакти з листа) і уточніть ситуацію.

Фішинг є однією з найпоширеніших кіберзагроз, і його уникнення вимагає комбінації належного розуміння та використання правильних технологій.

Найкращі практики для приватних осіб та підприємств:

– Освіта та навчання: На першому місці завжди повинна стояти освіта. Регулярні навчання з кібербезпеки допоможуть працівникам розпізнавати спроби фішингу.

– Технічні засоби: Використання відомого ліцензійного антивірусного програмного забезпечення та інших інструментів безпеки може значно знизити ризик потрапляння на шкідливі посилання.

– Багаторазова аутентифікація: Цей метод додає додатковий рівень захисту, навіть якщо зловмисники отримали доступ до ваших облікових даних.

Що робити якщо ви підозрюєте, що стали жертвою?

– Змініть паролі: Негайно змініть паролі від усіх облікових записів.

– Сканування на віруси: Проженіть систему за допомогою антивірусного програмного забезпечення.

– Повідомте: Якщо ви стали жертвою фішингу на робочому місці, негайно повідомте про це відділ IT.

Важливість постійного навчання – у світі кібербезпеки завжди відбуваються зміни. Нові загрози, такі як фішинг, виникають миттєво, тому постійне навчання та оновлення ваших знань є ключовим. Завдяки цьому ви завжди будете в курсі останніх трендів та методів захисту.

Тенденції:

– Зростання атак: На жаль, спроби фішингу постійно зростають. З появою нових технологій зловмисники вдосконалюють свої методики.

– Популярні методи: Основними цілями для фішерів залишаються електронні листи та SMS-повідомлення, але все частіше з’являються атаки через соціальні мережі та месенджери[4].

1.5 Висновки

У першому розділі кваліфікаційної роботи визначили актуальність питання кібербезпеки, визначили основні напрямки шахрайства та його різновиди, розглянули статистику за останні рокі та визначили найбільш потенційних жертв в залежності від віку та рівня знань про безпеку в інтернеті, розглянули схему на прикладі платформи оголошень “OLX” та визначили стандартні рекомендації щодо виявлення шахраїв по оголошенням та повідомленням. Зі статистики отримали данні про дії користувачів та їх рівень компетентності в поводженні з інцидентами кібершахрайств. Визначили основні причини зниження розвитку безпеки користування інтернетом.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Соціальна інженерія в фішингу

Соціальна інженерія стала невід'ємною частиною кібершахраїв. Мова йде про спеціальну методику маніпуляції, яка допомагає змусити людину віддати зловмисникам необхідні дані. Використовуючи людські слабкості, тобто емоції та природну поведінку жертви.

Соціальна інженерія – це мистецтво маніпулювання користувачами обчислювальної системи з метою розкриття конфіденційної інформації, яка може бути використана для отримання несанкціонованого доступу до комп'ютерної системи. Термін також може включати такі дії, як використання людської доброти, жадібності та цікавості для отримання доступу до будівель з обмеженим доступом або спонукання користувачів до встановлення бекдорного програмного забезпечення. Сьогодні існує чимало методів використання соціальної інженерії. В основі яких є маніпуляція людськими страхами, зацікавленістю або довірою. Жертвою соціальної інженерії можна стати як під час особистого спілкування, так і по телефону або через цифрові гаджети. Зловмисники можуть «маскуватися» під установи, яким довіряє людина.

Наприклад, прикидаючись представниками оператора мобільного зв'язку або працівниками банку, вони можуть надсилати електронні листи з додатком або посиланням, за яким людина має ввести свої особисті дані. Жертві також можуть додатково зателефонувати із проханням відкрити цей додаток або ж перейти за посиланням. Вважається, що таке спілкування додає ситуації чималої правдоподібності і зазвичай змушує людей відкривати вкладення. Знання трюків, які використовують хакери, щоб оманою змусити користувачів оприлюднити життєво важливу інформацію для входу, є фундаментальним для захисту комп'ютерних систем.

Злочінці для вдалого проведення атак використовують наступну схему, для підвищення ефективності та збору інформації:

– Збір інформації: це перший етап, на якому людина дізнається якомога більше про заплановану жертву. Інформація збирається з вебсайтів компаній, інших публікацій, а іноді й шляхом розмови з користувачами цільової системи.

– План атаки: зловмисники описують, як він/вона збирається здійснити атаку.

– Інструменти отримання: це комп'ютерні програми, які зловмисник використовуватиме під час атаки.

– Атака: використовуйте слабкі місця цільової системи.

– Використовуйте набуті знання. Інформація, зібрана під час тактики соціальної інженерії, як-от імена домашніх тварин, дати народження засновників організації тощо, використовується в атаках, наприклад підбір пароля.

Види моделей впливу на жертву:

Експлойт знайомства: користувачі менш підозрілі щодо знайомих їм людей. Зловмисник може ознайомитися з користувачами цільової системи до атаки соціальної інженерії. Зловмисник може взаємодіяти з користувачами під час їжі, коли користувачі курять, він може приєднатися, на соціальних заходах тощо. Це робить зловмисника знайомим користувачам. Припустімо, що користувач працює в будівлі, яка вимагає код доступу або картку для отримання доступу; зловмисник може стежити за користувачами, коли вони заходять у такі місця. Користувачі найбільше люблять тримати двері відкритими, щоб зловмисник зайшов, оскільки вони знайомі з ними. Зловмисник також може запитати відповіді на запитання, наприклад, де ви познайомилися зі своєю дружиною, ім'я вашого вчителя математики в середній школі тощо. Користувачі, швидше за все, розкриють відповіді, оскільки довіряють знайомому обличчю.

Обставини, що лякають: люди, як правило, уникають людей, які лякають оточуючих. Використовуючи цю техніку, зловмисник може прикинутися гарячою сваркою по телефону або зі спільником у схемі. Потім зловмисник може запитати у користувачів інформацію, яка буде використана для порушення безпеки системи користувачів. Користувачі, швидше за все, дають правильні відповіді, щоб

уникнути конфронтації з зловмисником. Цей прийом також можна використовувати, щоб уникнути перевірки на контрольно-пропускному пункті.

Фішинг: ця техніка використовує хитрість і обман для отримання особистих даних від користувачів. Соціальний інженер може спробувати видати себе за справжній веб-сайт, а потім попросити нічого не підозрюючого користувача підтвердити ім'я облікового запису та пароль. Цю техніку також можна використовувати для отримання інформації про кредитну картку або будь-яких інших цінних особистих даних.

Переслідування: ця техніка передбачає стеження за користувачами позаду, коли вони входять у заборонені зони. З людської ввічливості користувач, швидше за все, впустить соціального інженера в зону обмеженого доступу.

Експлуатація людської цікавості: використовуючи цю техніку, соціальний інженер може навмисно кинути заражений вірусом флеш-диск у місце, де користувачі можуть легко його підхопити. Користувач, швидше за все, підключить флешку до комп'ютера. Флеш-диск може автоматично запускати вірус, або користувач може спробувати відкрити файл із такою назвою, як Employees Revaluation Report 2022.docx, який насправді може бути зараженим файлом.

Експлуатація людської жадібності: використовуючи цю техніку, соціальний інженер може заманити користувача обіцянками заробити багато грошей в Інтернеті, заповнивши форму та підтвердивши свої дані за допомогою даних кредитної картки тощо.

Протидія моделям впливу з боку жертви:

Щоб протистояти експлойту знайомства, користувачів потрібно навчити не замінювати знайомство заходами безпеки. Навіть люди, з якими вони знайомі, повинні довести, що вони мають дозвіл на доступ до певних областей та інформації.

Щоб протистояти атакам залякування обставин, користувачі повинні бути навчені визначати методи соціальної інженерії, які виловлюють конфіденційну інформацію, і ввічливо відмовляти.

Щоб протистояти методам фішингу, більшість сайтів, таких як Google, використовують безпечні з'єднання для шифрування даних і доведення, що вони є тими, за кого себе видають. Перевірка URL може допомогти вам виявити підроблені сайти. Уникайте відповідей на електронні листи з проханням надати особисту інформацію.

Щоб протистояти небезпечним атакам, користувачі повинні бути навчені не дозволяти іншим використовувати їхній дозвіл безпеки для отримання доступу до зон обмеженого доступу. Кожен користувач повинен використовувати власний дозвіл доступу.

Щоб протистояти людській цікавості, краще надати підібрані флеш-диски системним адміністраторам, які мають перевірити їх на наявність вірусів чи іншої інфекції, бажано на ізольованій машині.

Щоб протистояти методам, які використовують людську жадібність, співробітники повинні бути навчені щодо небезпеки попадання на такі шахрайства[5].

2.2 Демонстрація, принцип дії і реалізація фішингових моделей

2.2.1 Демонстрація фішингової атаки методом фішингового сайта

Для реалізації одного з простих методів знадобиться ПК з ОС Windows, інтернет, середні навички роботи з ПК.

Для початку необхідно буде встановити ПЗ Gophish, ця програма є середовищем створення фішингових посилань та зберігання даних отриманих від жертв. Знайти цю програму можна на GitHub, вона знаходиться у вільному доступі та має відкритий код, це означає що більш розвинуті шахраї зможуть використовувати її та вдосконалювати, одним із популярних вдосконалень є перехід Gophish від її класичної бази даних SqlLite до MySQL. Сам фреймворк є

інструментом для створення, планування, моніторингу фішингових кампаній, створення і управління списками електронних адрес, шаблонів електронних листів і фішингових сторінок. Проте він не має функції SMTP-сервера. Тому для надсилання електронних листів потрібно підключати стороннє рішення.

Щоб запустити Gophish, нам потрібен будь-який Linux чи Windows сервер, загальнодоступний з мережі інтернет. Найпростіший варіант – це віртуальна машина на будь-якому популярному хмарному сервісі. Крім того, у таких провайдерів часто є безкоштовні «кредити», яких цілком достатньо для нашої демонстрації. Розгляньмо найпопулярніший з них – AWS.

Щоб створити нову віртуальну машину в AWS (див. рис. 2.1) , заходимо в консоль управління EC2 і натискаємо кнопку «Launch instances».

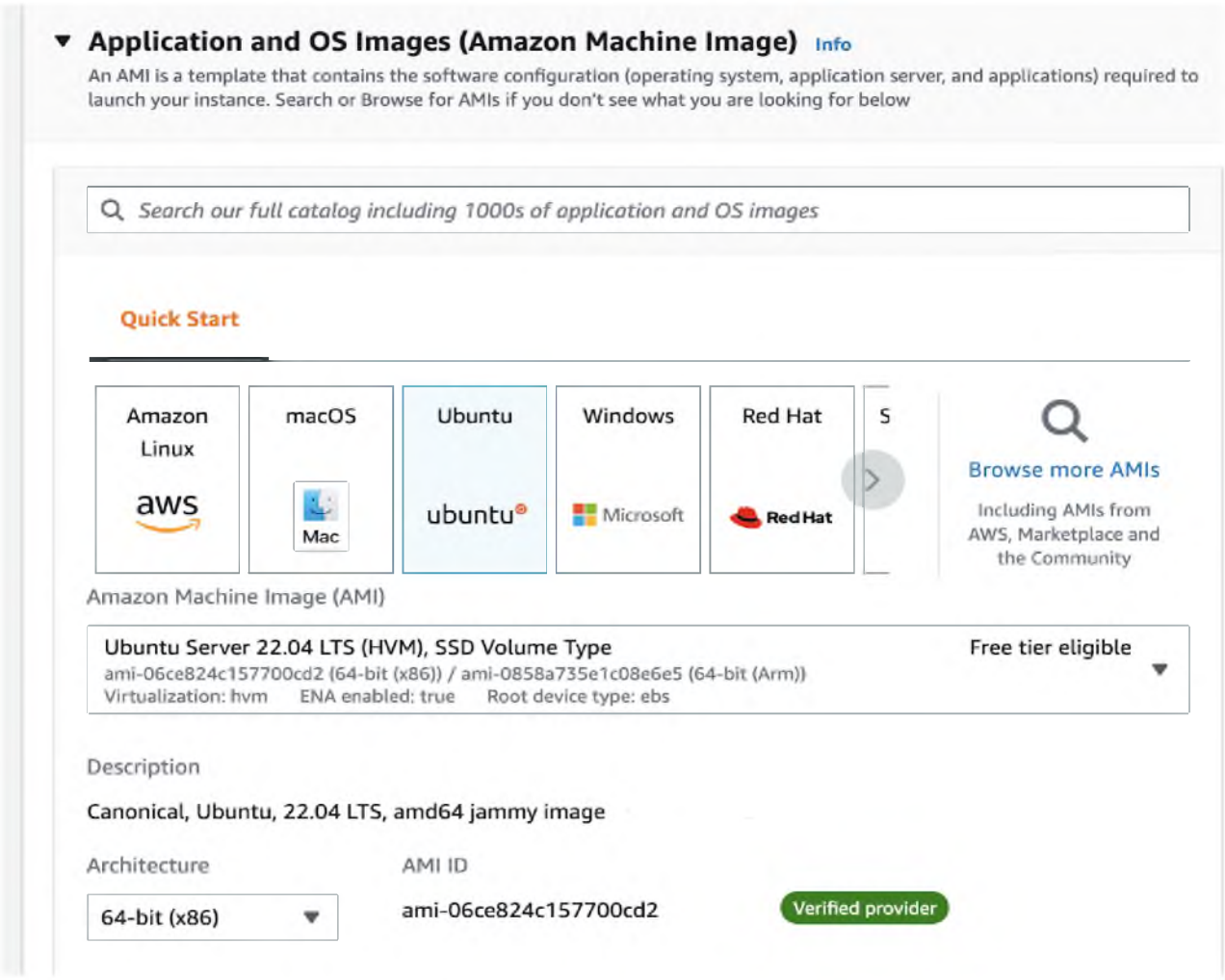

Рисунок 2.1 – Створення віртуальної машини в AWS

Для демонстрації оберемо операційну систему Ubuntu. При певних знаннях та вміннях можна використовувати інші операційні системи. Рекомендації щодо версій операційних систем відсутня, але слід пам'ятати, що надто старі версії можуть бути не стабільні до нових версій за стосунків, так само як свіжі версії які стали доступними впродовж останніх кількох тижнів, судячи з цих критеріїв для прикладу оберемо версії в діапазоні одного року.

Стосовно типу віртуальної машини, то достатньо буде обрати тип t2.micro. Цей розмір віртуальної машини сумісний із безкоштовними лімітами AWS. Також слід обрати наявну або створити нову пару ключів для підключення до машини по ssh-протоколу, як показано на рис. 2.2.

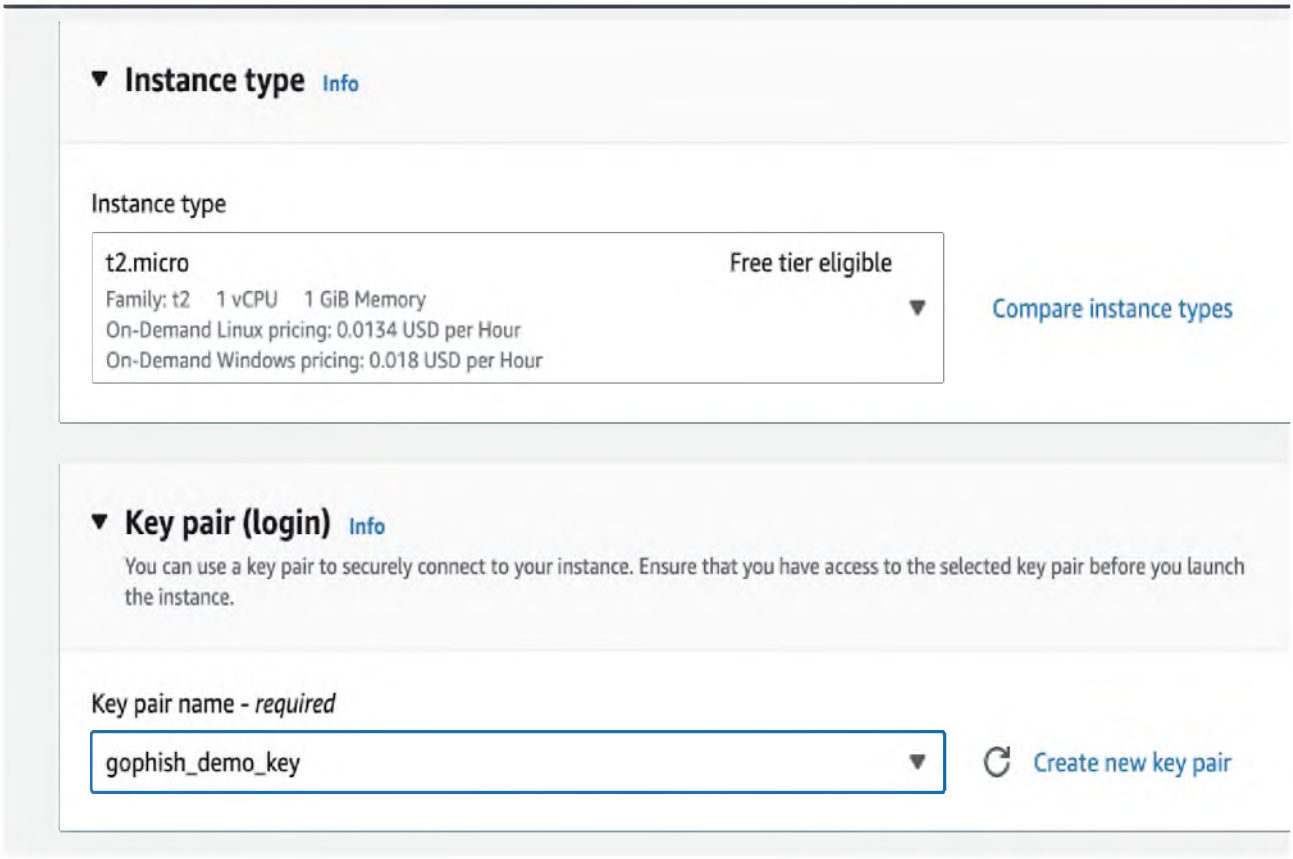

Рисунок 2.2 – Створення ключів доступу для віртуальної машини

У розділі Network Settings потрібно вказати мережеві правила для доступу до нашої віртуальної машини. Необхідно створити нову захищену групу, як показано на рис 2.3 з наступними правилами:

– Дозволити SSH трафік лише з нашої IP-адреси.

– Дозволити HTTP і HTTPS трафік з будь-якої адреси інтернету.

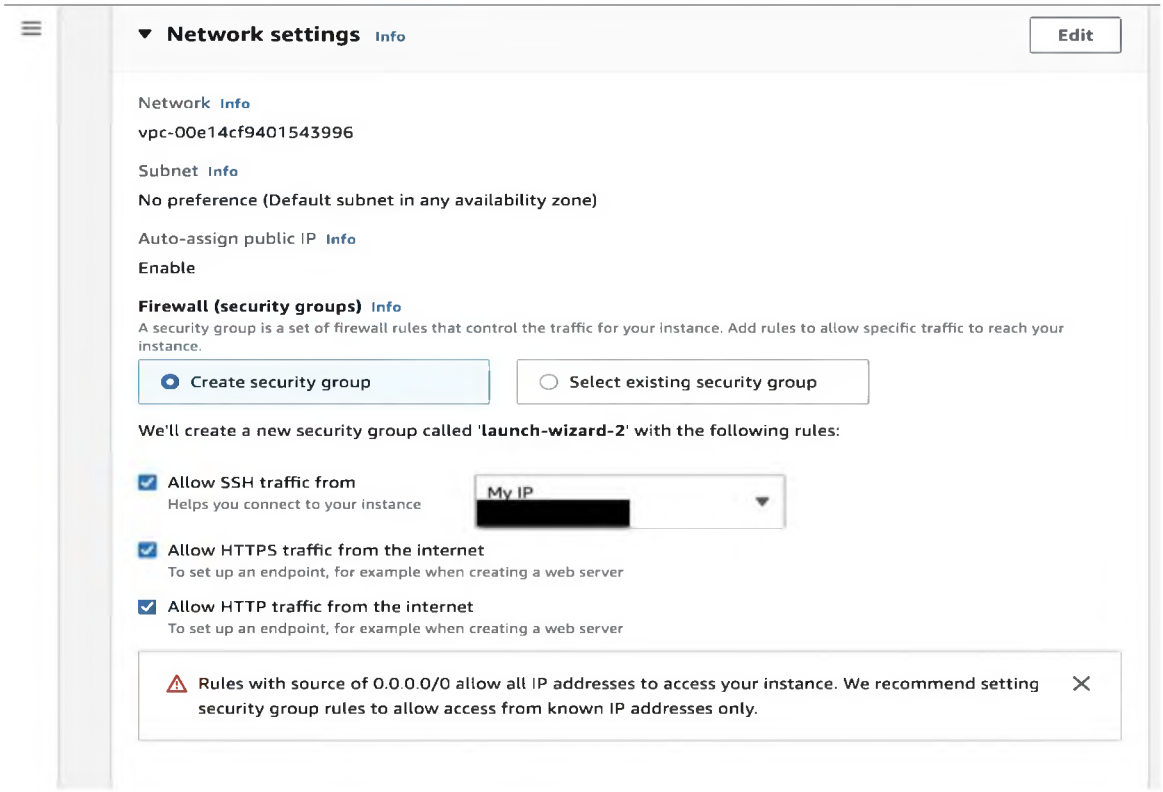

Рисунок 2.3 – Налаштування мережевих правил для віртуальної машини

Gophish-сервер буде хостити фішингові сторінки, а зловмисникам, щоб вони були доступні для потенційної «жертви». Повернемося до цих налаштувань пізніше, коли необхідно буде налаштовувати конфігурацію Gophish. Інші налаштування можна залишити за замовчанням.

Щоб під'єднатися до новоствореної машини необхідно обрати цей проект в списку адмінки EC2 і натиснувши кнопку «connect», як показано на рис 2.4.

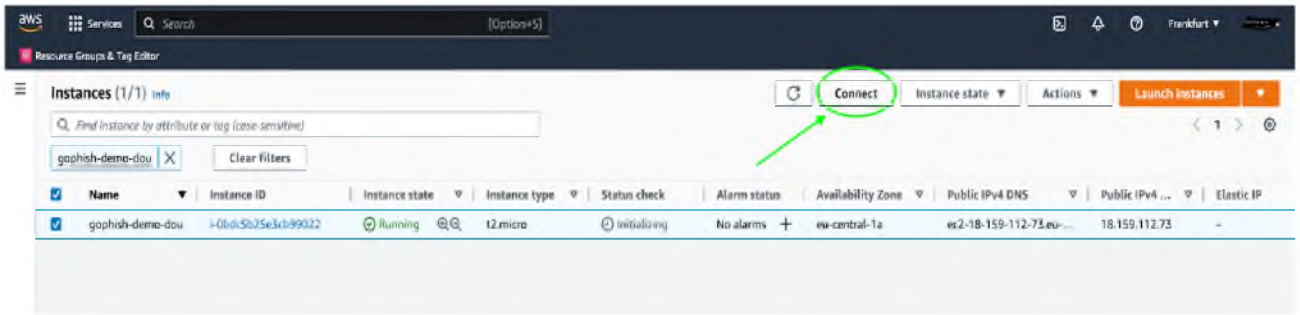

Рисунок 2.4 – Під'єднання до створеного проекту

Щоб під'єднатися через ssh, виконайте інструкції, вказані у вкладці *«SSH client»*. Також знадобиться ssh-ключ, обраний при створенні віртуальної машини. Запустити команду можна з теки, де знаходиться ключ. Таким спосіб виглядає наступним чином:

```
ssh -i "gophish_demo_key.pem" ubuntu@ec2-18-159-112-73.eu-central-1.compute.amazonaws.com
```

Найпростіший спосіб встановити Gophish – це звантажити архів з уже зібраним інструментом для вашої операційної системи. (Також можна використати Docker контейнер або клонувати репозиторій і зібрати проєкт самому). Створили віртуальну машину з операційною системою Ubuntu, тому нам потрібен архів зі збіркою під Linux.

Звантажуємо його наступною командою:

```
wget https://github.com/gophish/gophish/releases/download/v0.12.1/gophish-v0.12.1-linux-64bit.zip
```

Створимо нову теку і перейдемо у неї:

```
mkdir gophish
cd gophish
```

Тепер розпаковуємо зміст завантаженого архіву в поточну теку:

```
unzip ../gophish-v0.12.1-linux-64bit.zip
```

Перевірмо розпакований з архіву вміст поточної теки:

```
ls
```

Повинні побачити наступні файли й теки, див рис.2.5:

Рисунок 2.5 – Перевірка вмісту теки з встановленого архіву

Тека *db* містить конфігурації й міграції для баз даних. В теках *static* і *templates* містяться файли UI-інтерфейсу. *gophish* – це бінарний файл, який будемо запускати. *config.json* – це файл, в якому міститься конфігурація інструменту. Перевірмо його вміст, див рис. 2.6.

```
cat ./config.json
```

```
ubuntu@ip-172-31-28-65:~/gophish$ cat ./config.json
{
        "admin_server": {
                "listen_url": "127.0.0.1:3333",
                "use_tls": true,
                "cert_path": "gophish_admin.crt",
                "key_path": "gophish_admin.key",
                "trusted_origins": []
        },
        "phish_server": {
                "listen_url": "0.0.0.0:80",
                "use_tls": false,
                "cert_path": "example.crt",
                "key_path": "example.key"
        },
        "db_name": "sqlite3",
        "db_path": "gophish.db",
        "migrations_prefix": "db/db_",
        "contact_address": "",
        "logging": {
                "filename": "",
                "level": ""
        }
}
```

Рисунок 2.6 – Конфігурації “Gophish” з файлу config.json

Розділи конфігурації *admin_server* і *phish_server* містять відповідно налаштування «адмінки» (де зловмисник створив і запустив кампанії) і фішингового сервера (відповідає за хостинг фішингових сторінок, які додаються через ту ж адмінку). З цих налаштувань бачимо, що наразі «адмінка» доступна лише безпосередньо на віртуальній машині через порт 3333, а фішинговий сервіс доступний на 80 порту з мережі. Щоб спростити демонстрацію і зробити адмінку

Gophish доступною поза віртуальною машиною, змінюємо «admin_server.listen_url»: «0.0.0.0:3333». Це зручно зробити в консольному редакторі nano.

```
nano ./config.json
```

Робимо зміни. Щоб вийти з редактора і зберегти зміни, натискаємо комбінацію control + X, і отримуємо як показано на рис. 2.7.

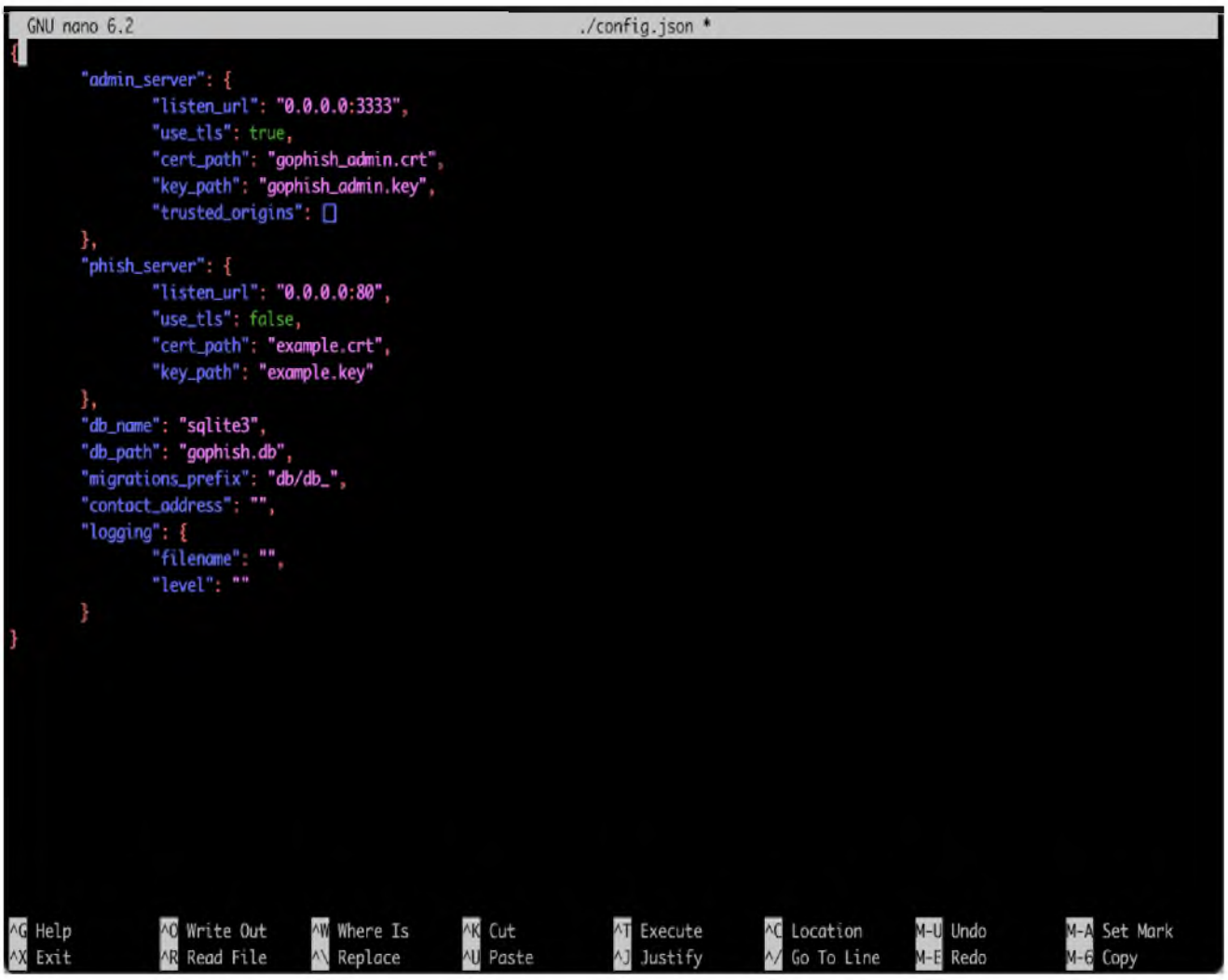

Рисунок 2.7 – Редагування конфігурацій “Gophish” з файлу config.json

В реальності, є необхідність, щоб фішинговий сервер віддавав сторінки по HTTPS, що буде викликати у «жертви» більше довіри. Саме в *config.json* файлі ви зможете змінити порт і вказати файли ssl-сертифікату. Як альтернатива, можна використати cloudflare flexible ssl, коли комунікація між браузером і cloudflare

буде захищеною, а між cloudflare і фішинговим сервером з'єднання буде відбуватися по HTTP.

Щоб дозволити доступ до адмінки Gophish поза віртуальною машиною, нам також потрібно відредагувати правила вхідного трафіку віртуальної машини. Для цього заходимо у налаштування віртуальної машини, на закладці Security переходимо у відповідну захищену групу(див. рис. 2.8).

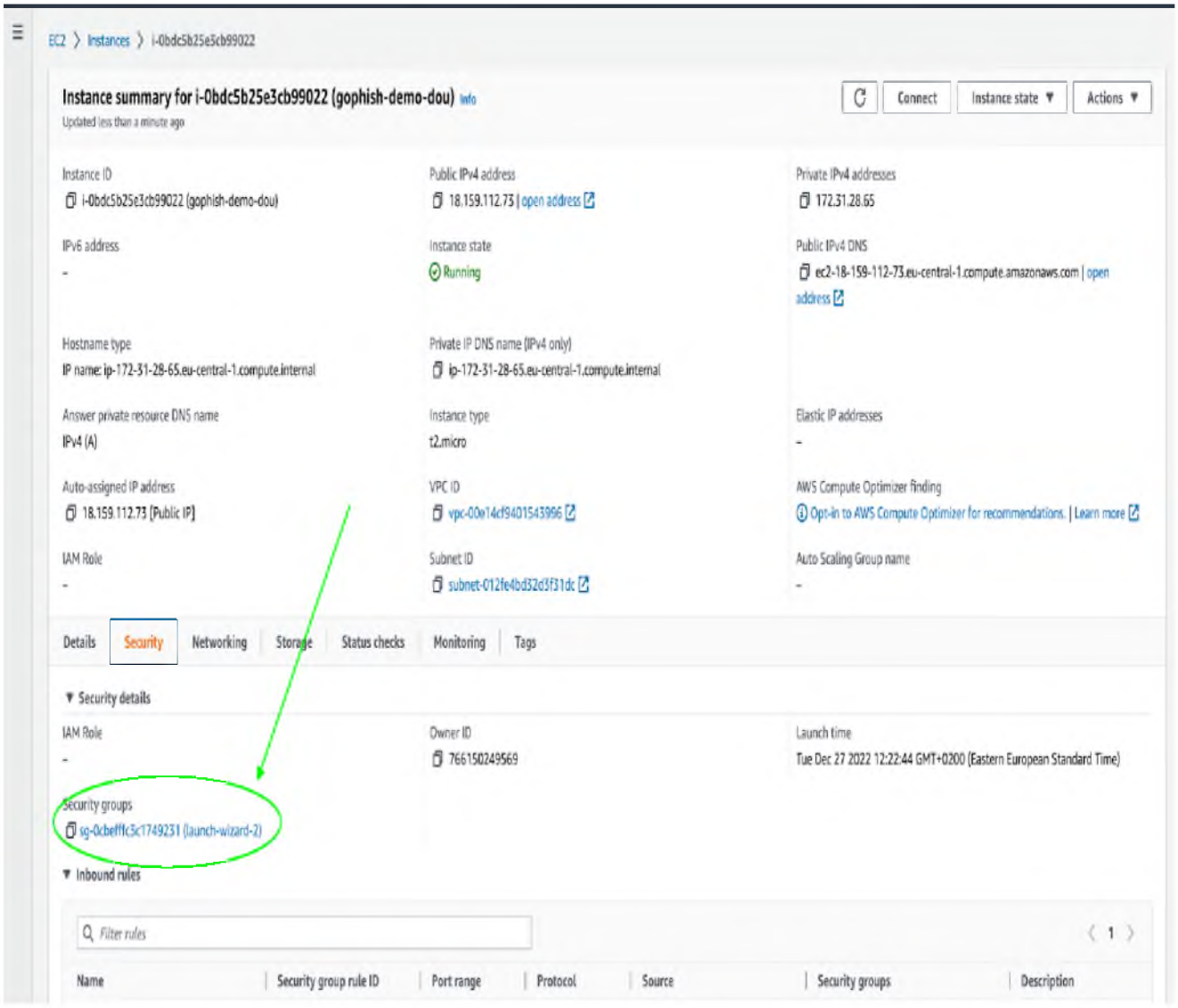

Рисунок 2.8 – Кнопка переходу до редагування захищеної групи

На сторінці захищеної групи натискаємо на кнопку *«Edit inbound rules»*, як показано на рис.2.9.

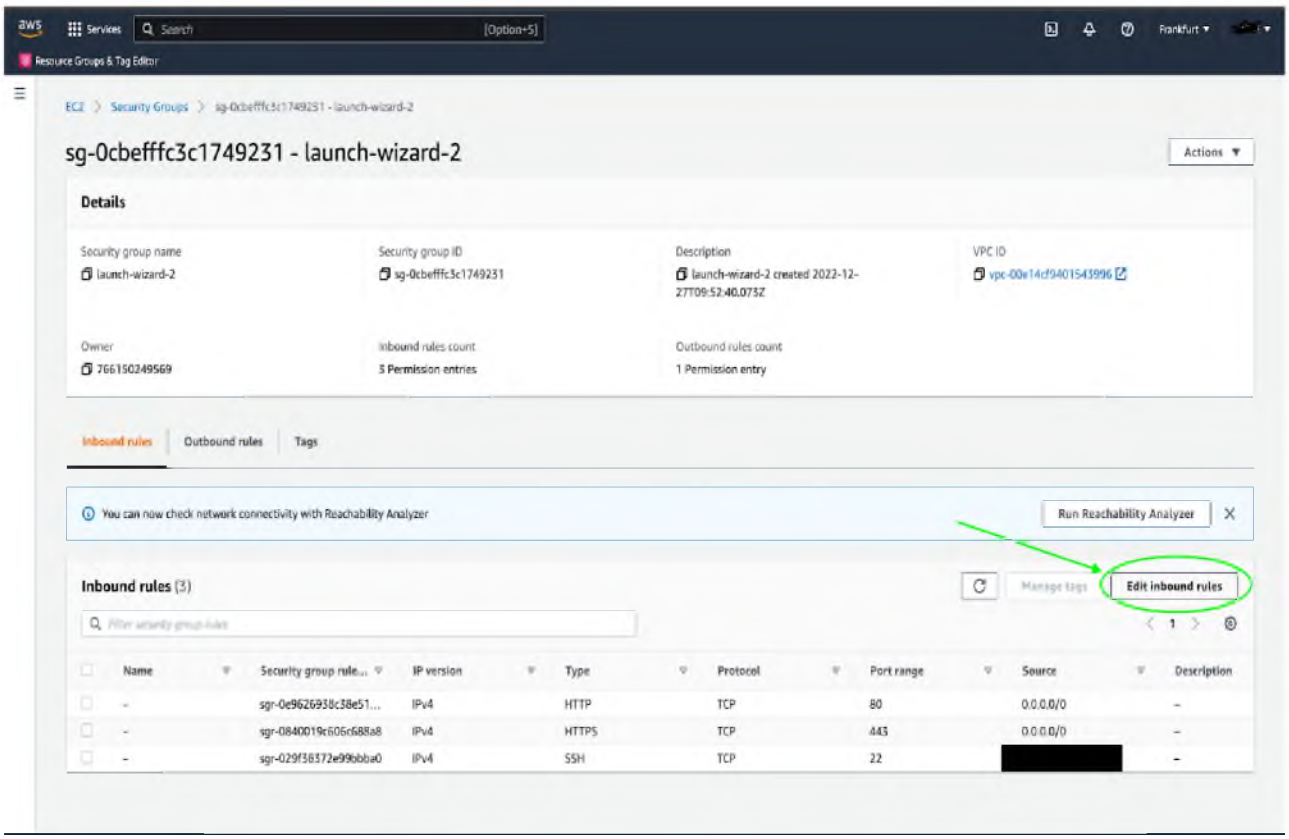

Рисунок 2.9 – Кнопка налаштування вхідних правил

У цій групі обираємо налаштування адреси підключення, обираємо створення з моєї адреси, після чого налаштування самостійно отримає та заповнить поле вашими даними, як на рис.2.10 .

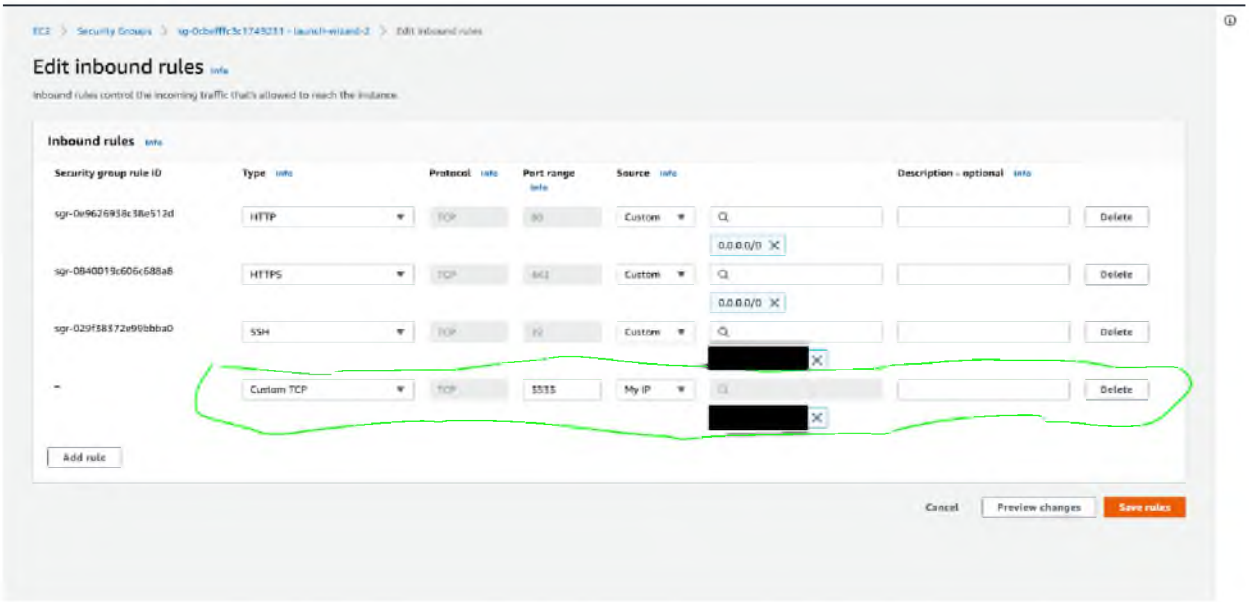

Рисунок 2.10 – Поле правила доступу за вхідним адресом

Повертаємося до нашої віртуальної машини. Потрібно зробити файл gophish виконуваним. Для цього запускаємо наступну команду:

```
chmod +x gophish
```

Тепер можемо запустити наш сервер (запуск із sudo потрібний для того, щоб приєднатися до 80 привілейованого порту). Важливий нюанс: якщо запускаємо сервер таким чином, то при закінченні ssh-сесії Gophish перестане працювати, що недопустимо в реальних умовах. Швидше за все знадобиться запустити інструмент як сервіс і під окремим користувачем. Але для спрощення демонстрації пропустимо це.

```
sudo ./gophish
```

В консолі бачимо повідомлення з паролем для admin користувача. Важливо зберегти цей пароль і використати для першого логіну в «адмінку» Gophish. Також бачимо повідомлення про старт фішингового серверу на 80 порту і старт адмінки на 3333 порту, див нижче рис 2.11.

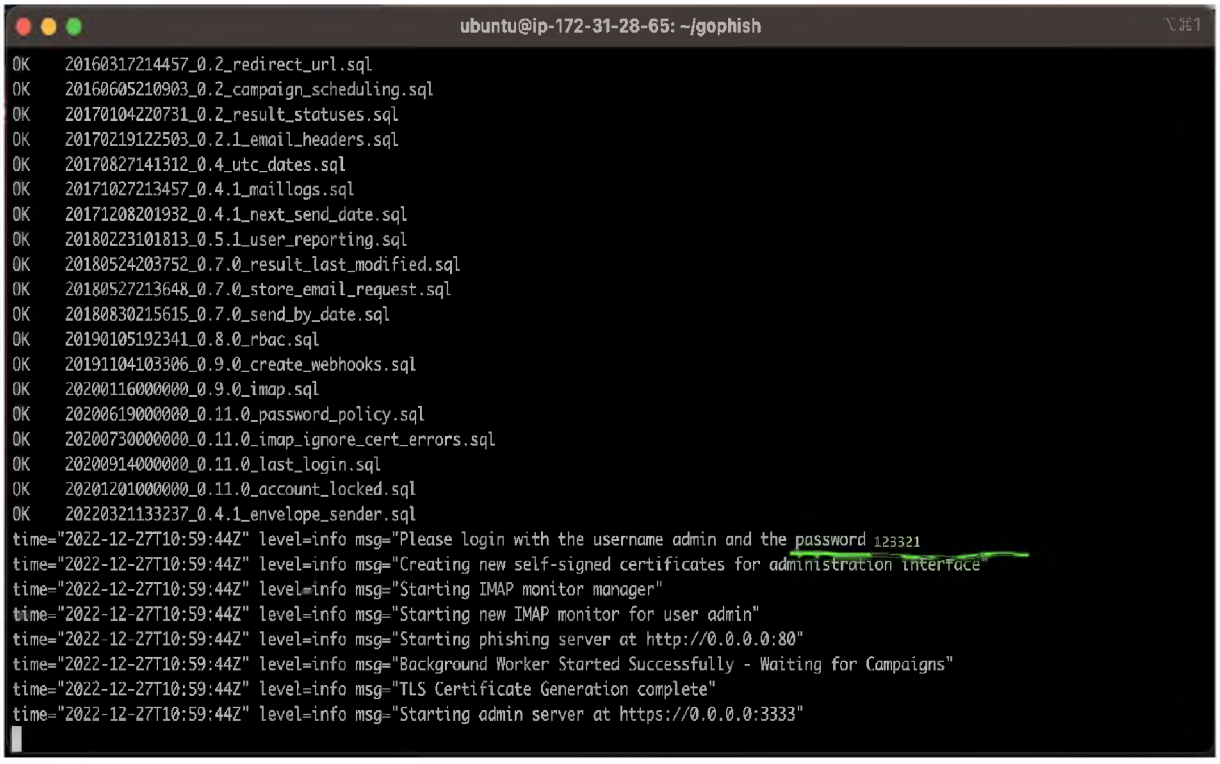

Рисунок 2.11 – Старт сервера та перші дані для входу

Спробуймо відкрити адмінпанель в браузері. Для цього нам потрібна IP-адреса нашої віртуальної машини (її можна глянути у панелі управління EC2). Отже, в адресному рядку вводимо https://[ip віртуальної машини]:3333 (в нашому тестовому випадку https://18.159.112.73:3333), як можна це побачити на рис 2.12.

Рисунок 2.12 – Знаходження адреси у вкладці “рішення”

Після цим маніпуляцій, тестовий Gophish-сервер працює. Для підключення слідвикористати тимчасовий пароль із попереднього кроку, щоб потрапити в «адмінку». При першому логіні система попросить змінити пароль на новий постійний (рис. 2.13). Після успішної авторизації побачимо інтерфейс Gophish.

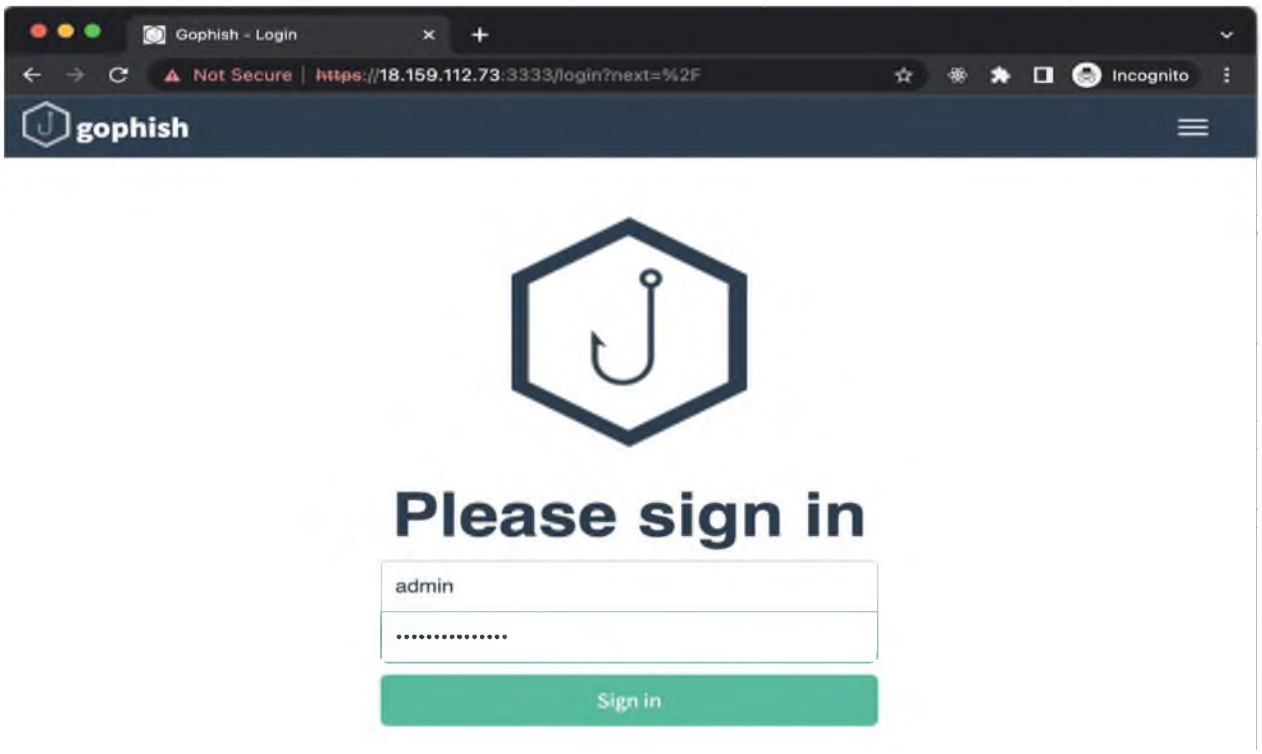

Рисунок 2.13 – Авторизація в Gophish

Запуск першої кампанії з Gophish

Спробуємо на прикладі зімітувати фішингову атаку і розберемося з функціоналом Gophish. Зловмисник хоче отримати доступ до акаунтів користувачів сервісу WordPress.org. Перше, що зловмиснику потрібно – це підставна фішингова сторінка, наприклад, з формою логіна. З неї й розпочнемо підготовку.

Розміщення сторінки

Цей розділ дозволяє створити HTML-сторінки, на які при переході із фішингового посилання потрапляє «ціль». Функціональність лендінгових сторінок дозволяє зберігати надіслані користувачем дані, що значно спрощує підготовку. Додаємо нову сторінку (рис 2.14).

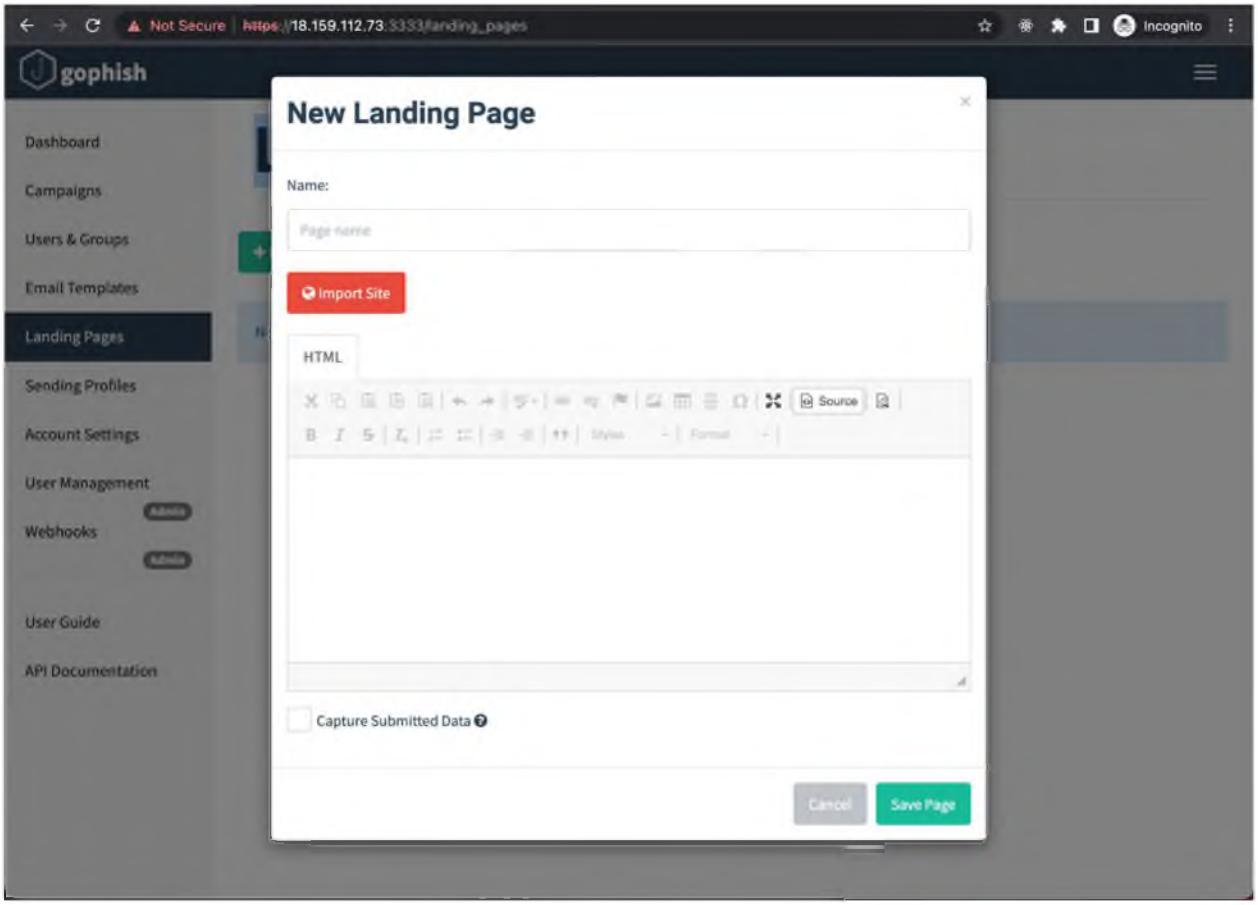

Рисунок 2.14 – Створення нової сторінки

У формі створення Landing Page є можливість додати HTML-сторінки, або ж спробувати імпортувати сторінку з сайту. Імпорт сторінки не завжди спрацює

(наприклад, якщо форма рендериться на клієнтській стороні, а не віддається сервером, як статична сторінка). Спробуймо імпортувати сторінку логіну https://login.wordpress.org з сайту WordPress.org. Натискаємо кнопку *«Import Site»*, потім у формі, яка з'явилася, вставляємо посилання на сторінку логіна і натискаємо *«Import»* див. рис. 2.15.

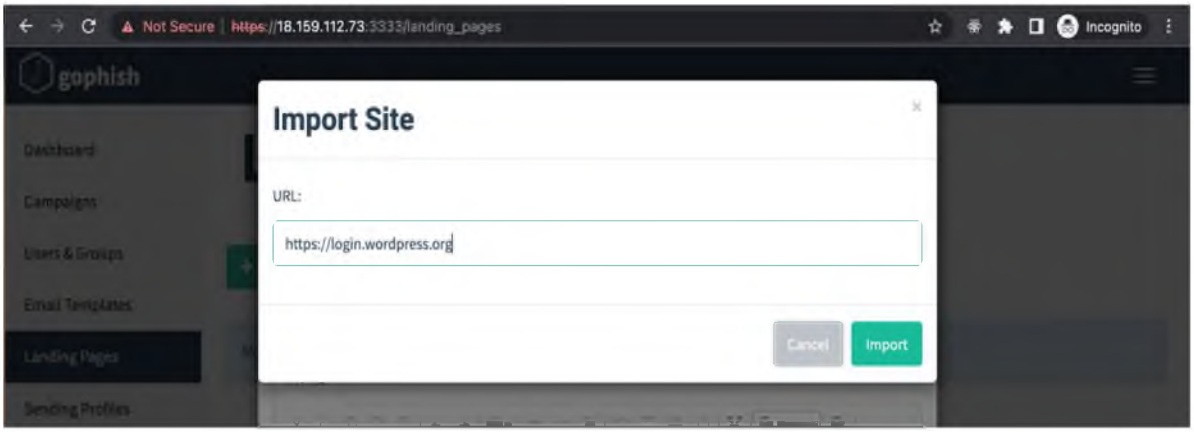

Рисунок 2.15 – Імпортування сторінки

Після того, як форма імпорту закрилася, бачимо у візуальному редакторі копію сторінки логіну з WordPress.org. На перший погляд – досить непогано. За потреби можна відредагувати цю сторінку, переключившись у режим редагування HTML (рис. 2.16).

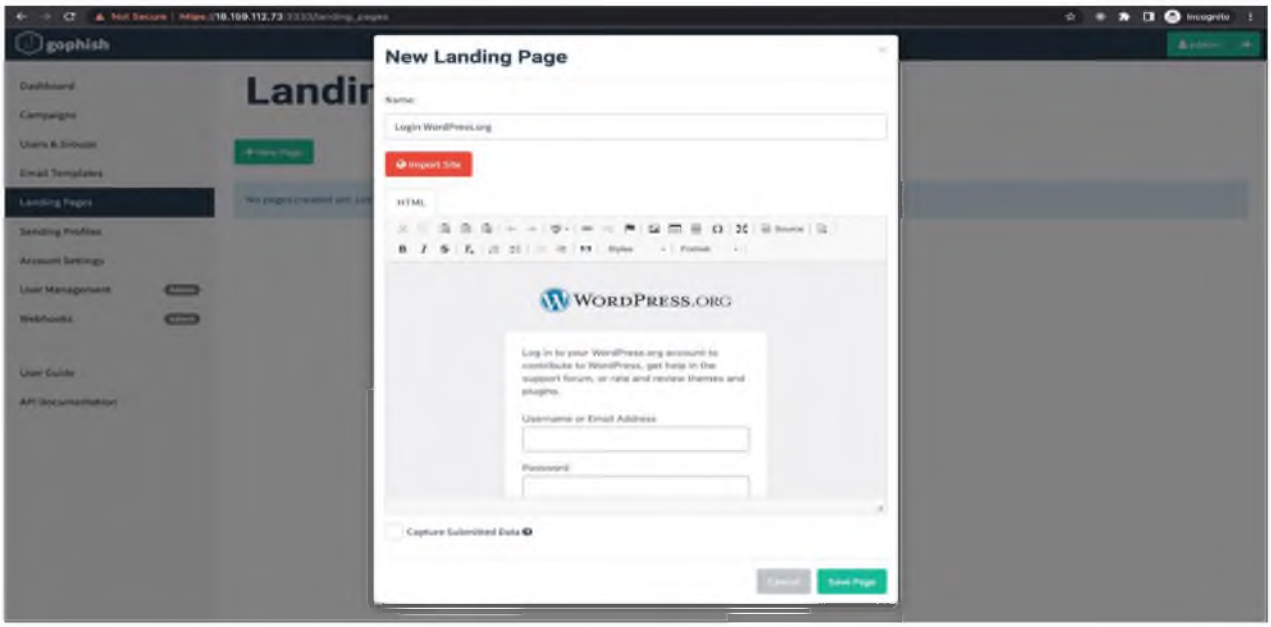

Рисунок 2.16 – Макет фейкової сторінки авторизації

Оскільки зловмисник зацікавлений у логіні та паролі користувачів, ставимо галочку *«Capture Submitted Data»* і також ставимо позначку навпроти нового пункту, який з'явиться, *«Capture Passwords»*. Оскільки зловмисник не хоче викликати підозр навіть коли користувач уже ввів свої дані, вкажемо, щоб «ціль» перенаправлялась на сторінку профілю.

Для порівняння з іншими схожими продуктами існує різниця в реалізації захоплення паролю, певні інструменти можуть автоматично змінювати пароль або поштову адресу ново викрадених даних, щоб повністю заволодіти персональними даними, а інші програмні продукти можуть маскуватися, збирати інформацію для доступу до сторінки і ніяк себе не виявляти (рис.2.17).

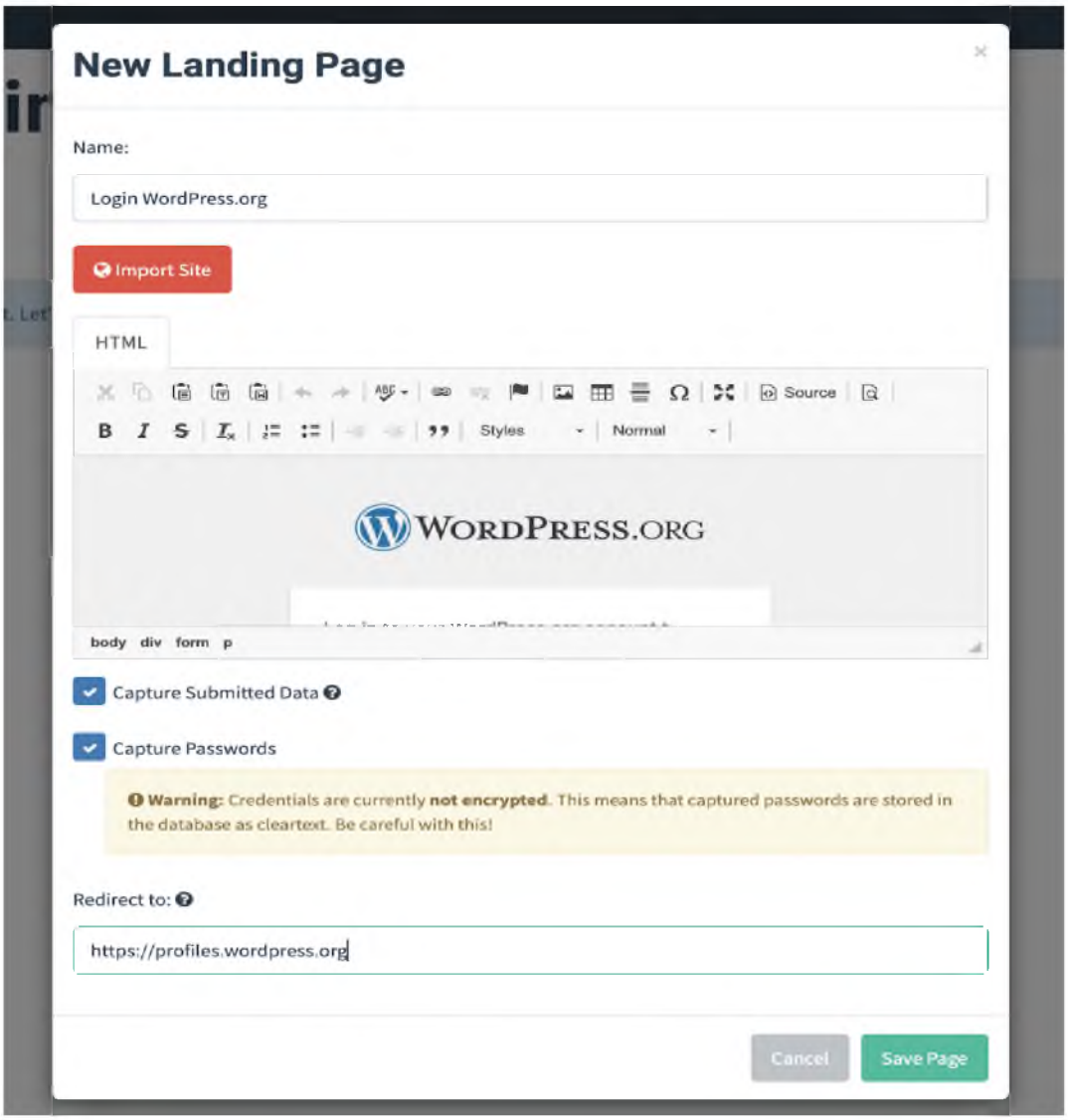

Рисунок 2.17 – Налаштування фейкової сторінки авторизації

Електронне сповіщення

Наступний крок у плануванні атаки – це підготовка фішингового листа, який має привести користувача на уже створену нами сторінку. Перевіривши стиль електронного листа, який має вигляд як переставлено на рис. 2.18, який приходить при зміні пароля на WordPress.org, бачимо, що повідомлення містить простий текст без стилів і зображень, що значно спрощує наше завдання.

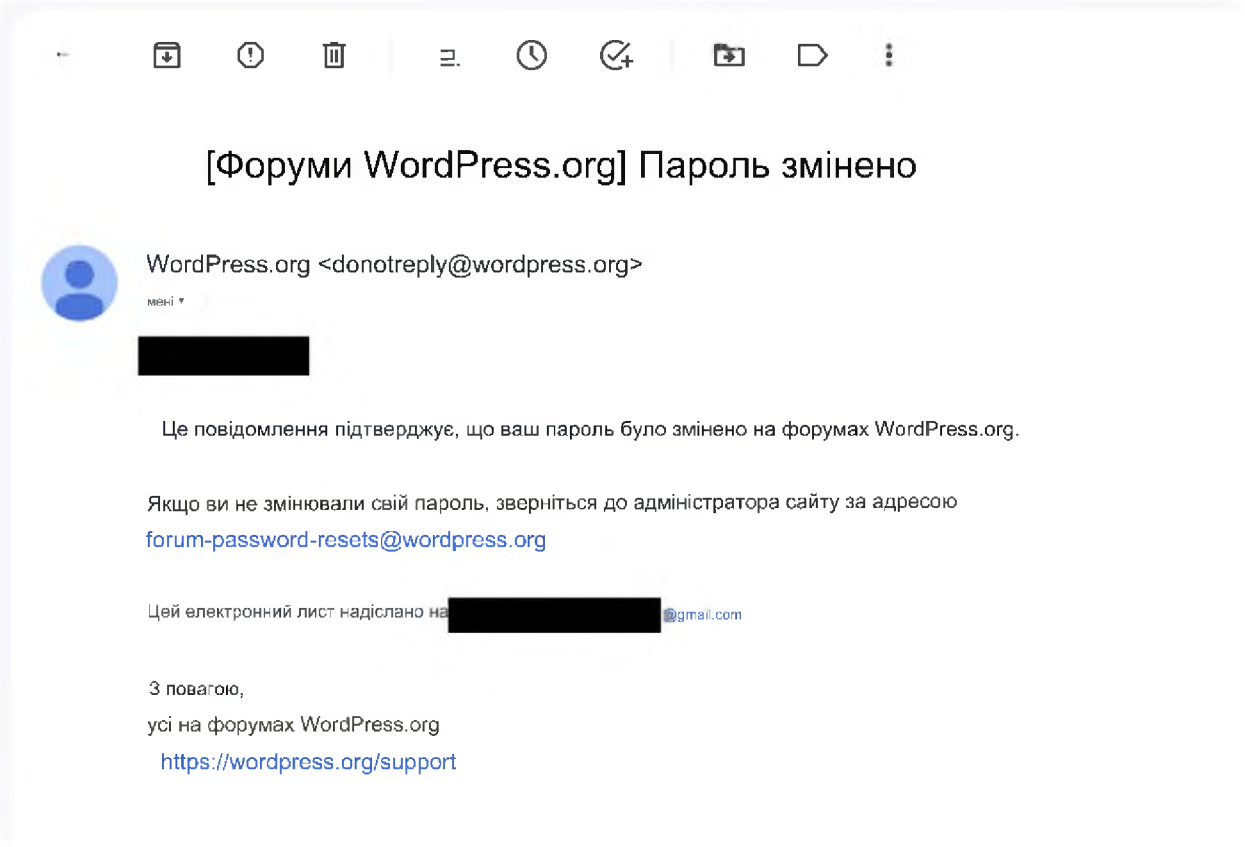

Рисунок 2.18 – Лист відновлення паролю

Зробити лист, який змотивує користувача перейти на фішингову сторінку і ввести свої облікові дані. Наприклад, повідомити, що через недавній інцидент на платформі користувачу потрібно перелогінитися, щоб зберегти доступ до свого профілю. Знову ж таки, для реальної кампанії потрібно проявити більше винахідливості й докласти більше зусиль.

Цікавою функціональністю email-шаблонів є можливість використовувати змінні, які будуть підставляти відповідні значення у конкретний лист (наприклад,

ім’я чи email) на рис 2.19 показано як він виглядає. Також є можливість імпортувати уже наявний лист.

Ставимо галочку *«Add tracking image»*, щоб мати статистику про відкриття емейлу потенційними «жертвами».

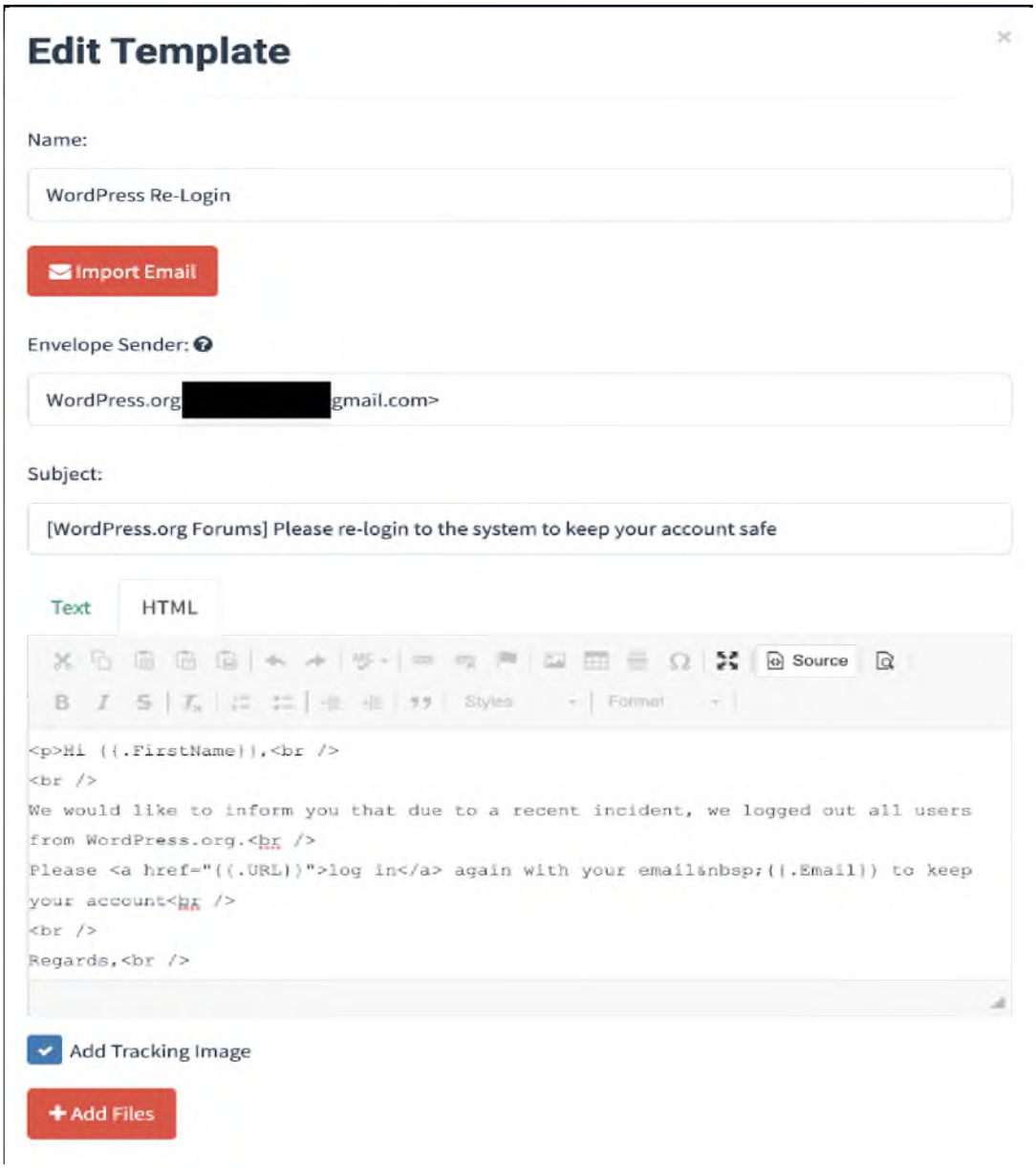

Рисунок 2.19 – Створення фішингового листа

Також Gophish дає можливість додавати прикріплені файли до шаблону листа. Але роботу з атачментами залишимо, оскільки в реальному листі немає необхідності це робити, якщо підробляти листи з атачментами, це займе лише трохи більше часу.

Надсилання профілю

Наступне, що нам потрібно, це SMTP-сервер, який надсилатиме електронні листи. Сам Gophish не вміє цього робити. З демонстраційною метою можемо використати SMTP будь-якого популярного сервісу email-розсилок (див. на рис.2.20), наприклад SendGrid. У SendGrid також є безплатні ліміти, що чудово підходить для тесту. Після реєстрації дані SMTP-сервера SendGrid можна знайти на сторінці Email API -> Integration Guide -> SMTP Relay.

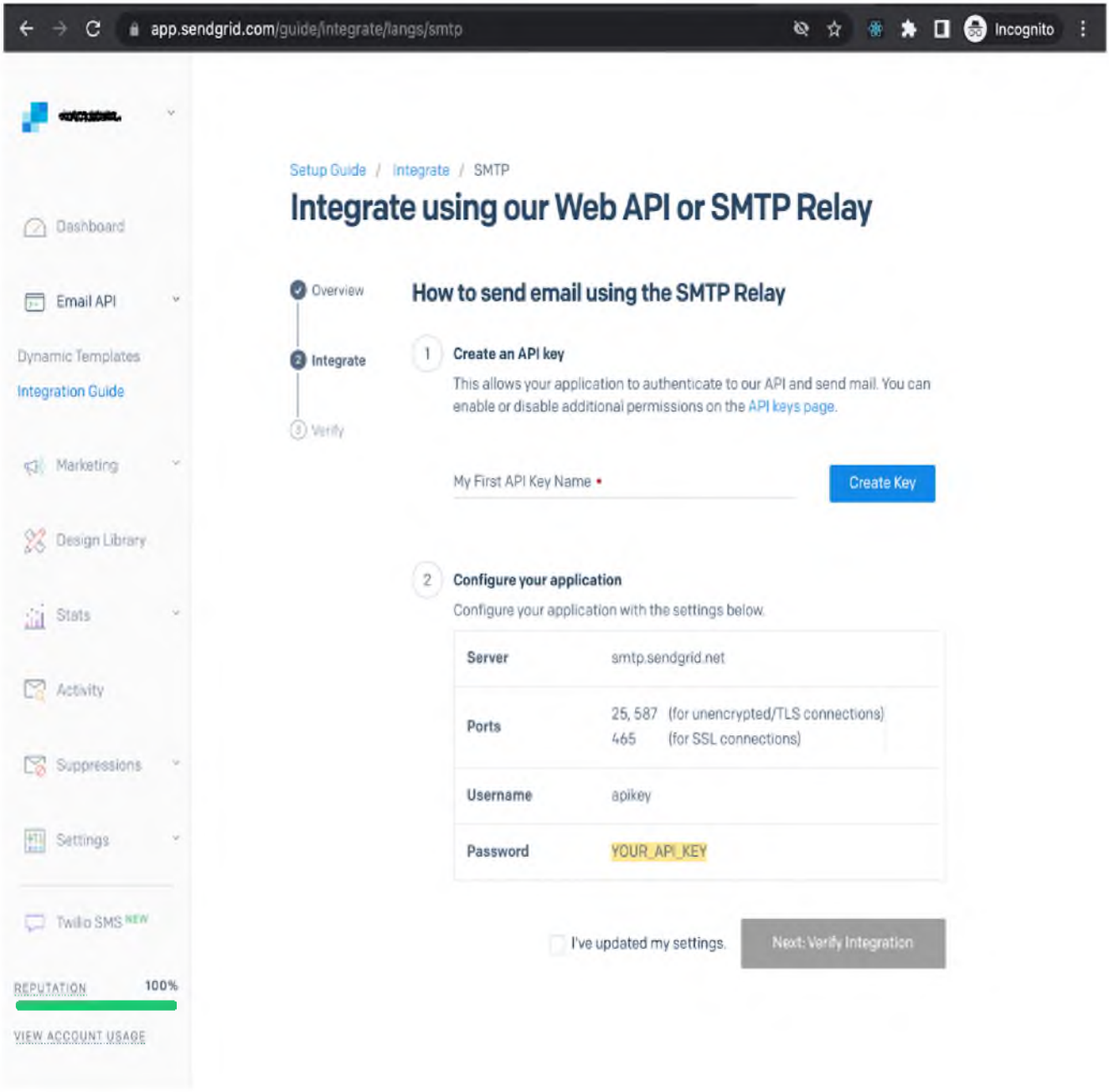

Рисунок 2.20 – Налаштування розсилки фішингових листів

Використаємо цю інформацію при додаванні Sending Profile.

Ці налаштування необхідні для пасивного пошуку жертв, до цього лист, дуже схожий на оригінальний, додає впевненості жертві, що ця інформація є достовірною і їй треба захистити свій профіль від зловмисників (рис.2.21)

Згідно статистики, фішингові листи є найбільш популярним пасивним методом у зборі інформації та заманювання жертв.

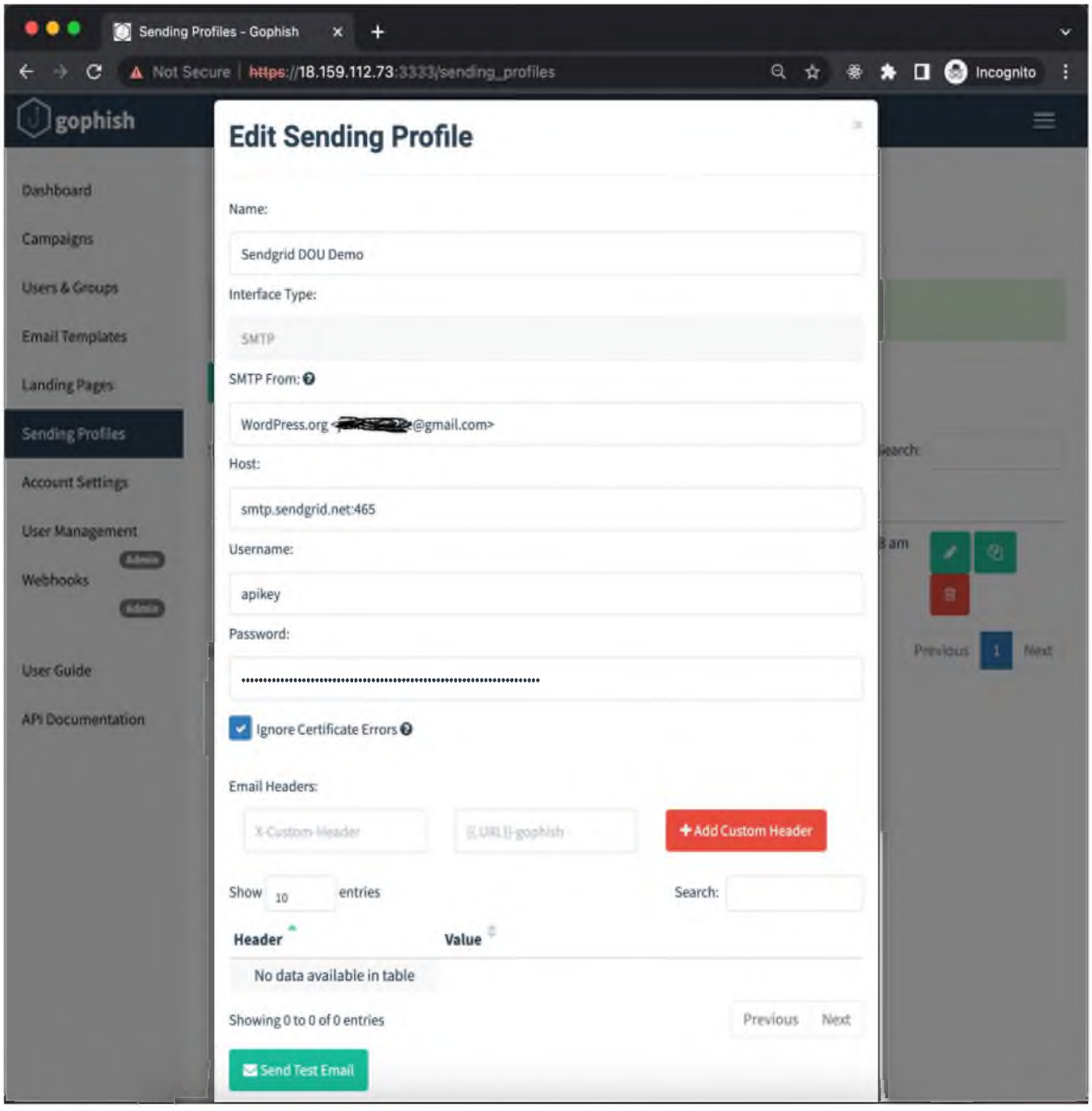

Рисунок 2.21 – Налаштування посилань фішингових листів до Gophish

Користувачі та групи. Останнім кроком потрібно додати список електронних пошт, які будуть ціллю атаки. У формі створення нової групи можна

додавати емейли по одному або імпортувати групу електронних пошт за допомогою csv-файлу.

Цей крок можна зробити багатьма методами, один із яких це самостійне збирання адрес через відкриті джерела, наприклад сам WordPress на форумі видає більшість адрес користувачів, якщо вони залишили можливість переглядати свою електронну адресу, інший метод збирання масивів даних за допомогою сторонніх застосунків, наприклад автоматизатора пошуку адрес чи використання сторонніх масивів даних знайдених або придбаних в інтернеті (рис. 2.22).

Оскільки в нашому прикладі є певний ліміт на розсилку, нам підійде метод самостійного пошуку електронних адрес, щоб не вичерпати ліміт на можливі неіснуючі або покинуті адреси.

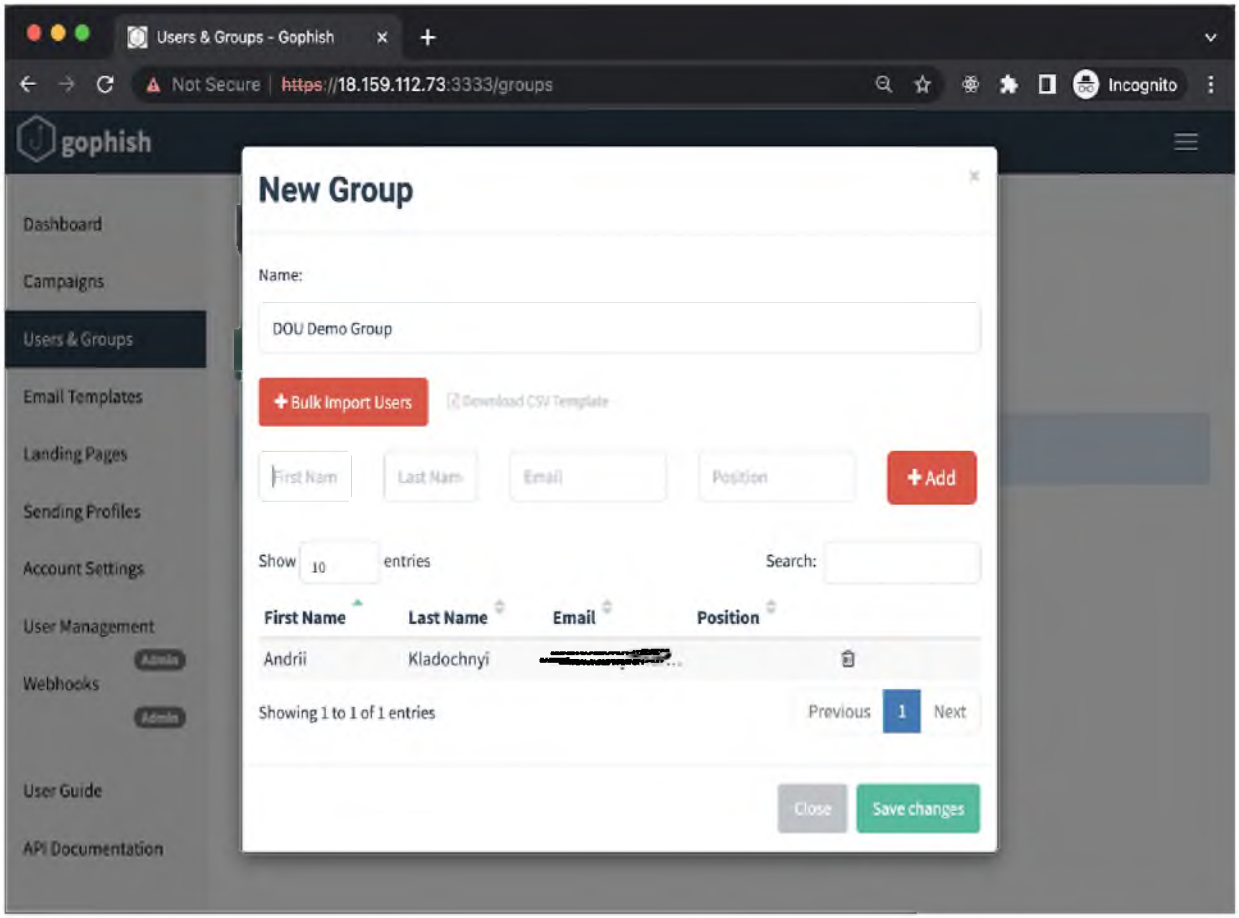

Рисунок 2.22 – Завантаження тестового списку розсилання фішингових листів

Компанії. Нарешті зловмисник готов до запуску першої кампанії. На формі створення обираємо додані на попередніх кроках email template, landing page,

sending profile і групу емейлів для розсилки. Крім цього, нам потрібно вказати URL, де буде хоститися фішингова сторінка. В цьому випадку вказуємо IP-адресу віртуальної машини, де розгорнули Gophish («Public IPv4 address» в панелі управління EC2).

В реальності потрібно отримати статичну адресу для віртуальної машини й прив'язати власний домен. Також можна запланувати час старту розсилки. Якщо вказати час *«Send Emails By»*, Gophish розподілить надсилання фішингових повідомлень між цими двома проміжками часу. Коли зловмисник готовий, він натискає кнопку *«Launch Campaign»* (рис.2.23).

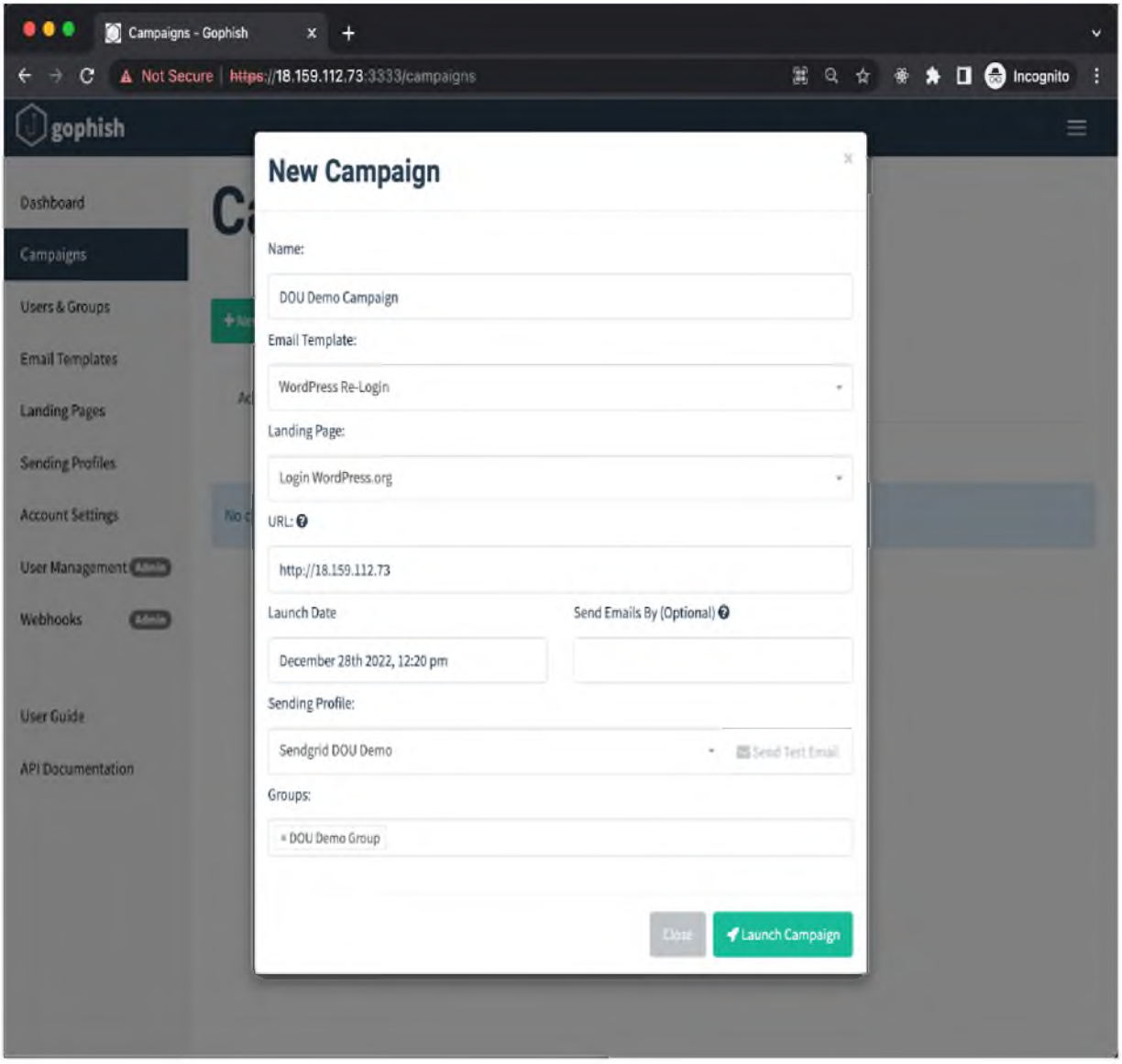

Рисунок 2.23 – Запуск компанії в Gophish

Після запуску можемо спостерігати детальну інформацію про перебіг кампанії. Кількість надісланих листів, кількість відвідувачів фішингової сторінки, захопленні данні для входу, тощо.

Заходимо на електронну пошту, яка була вказана як «ціль» і перевіримо, чи отримали електронний лист (рис. 2.24).

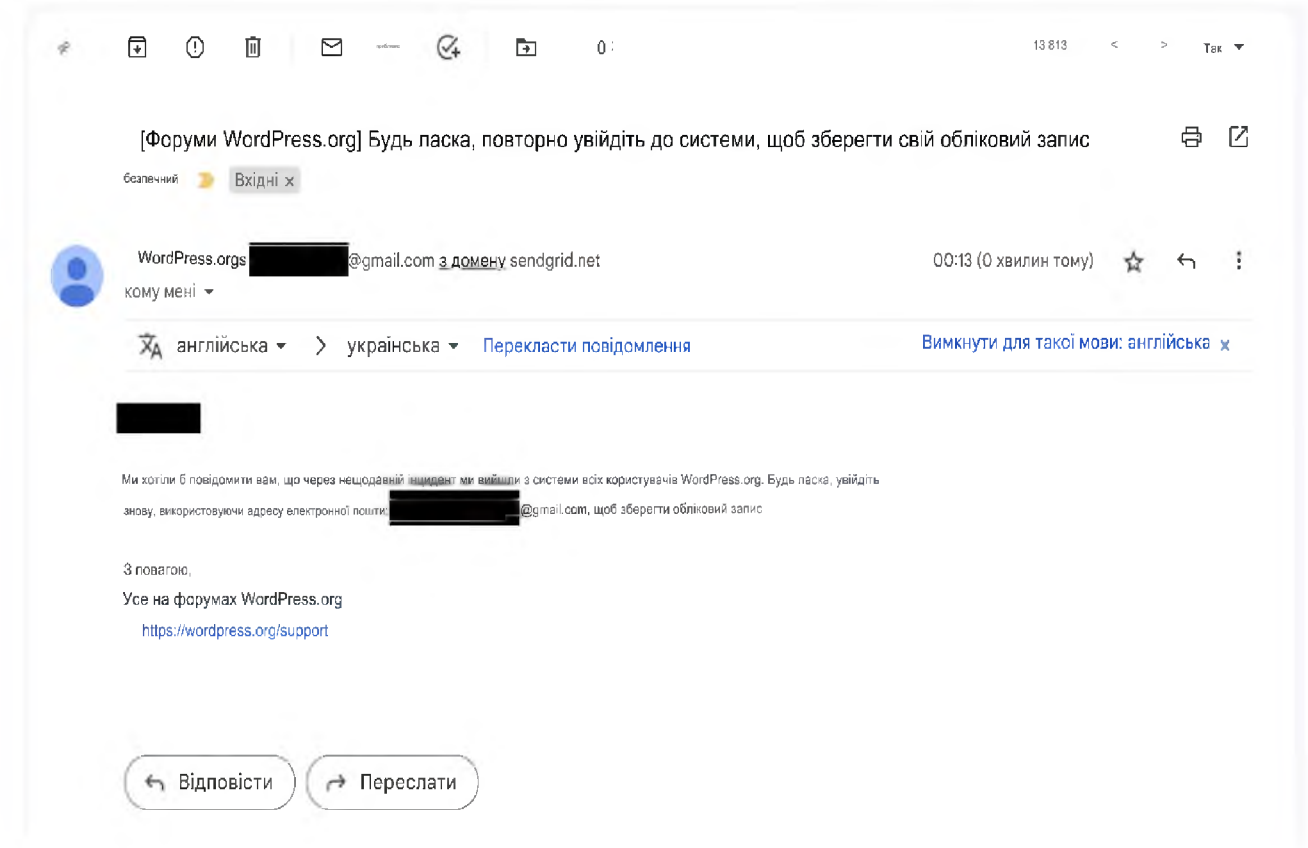

Рисунок 2.24 – Лист фішингової компанії

Здається, це дійсно щось важливе! При переході на посилання, вказане у листі, потрапляємо на сторінку, яка дуже схожа на справжню сторінку логіна WordPress.org.

Не довго думаючи, «жертва» вводить логін і пароль, і після натискання кнопки «*Log In*» потрапляє на сторінку свого профілю (це було вказано у налаштуваннях Landing Page). Якщо користувач був залогінений на сайті, то він може навіть нічого не помітити.

У разі коли жертва не авторизована на офіційному сайті, її направить на сторінку авторизації (рис. 2.25), де треба буде заново вводити данні, більшість

людей це ставить під сумніви, інші гадають на певні перебої в роботі інтернету, сервера чи других речей. У цьому випадку є шанс що жертва здогадається і змінить пароль, у цьому випадку зловмисник втратить доступ до особистого кабінету жертви, але є можливість, що пароль може бути уніфікованим для доступу до інших сайтів, наприклад до пошти або соціальних мереж.

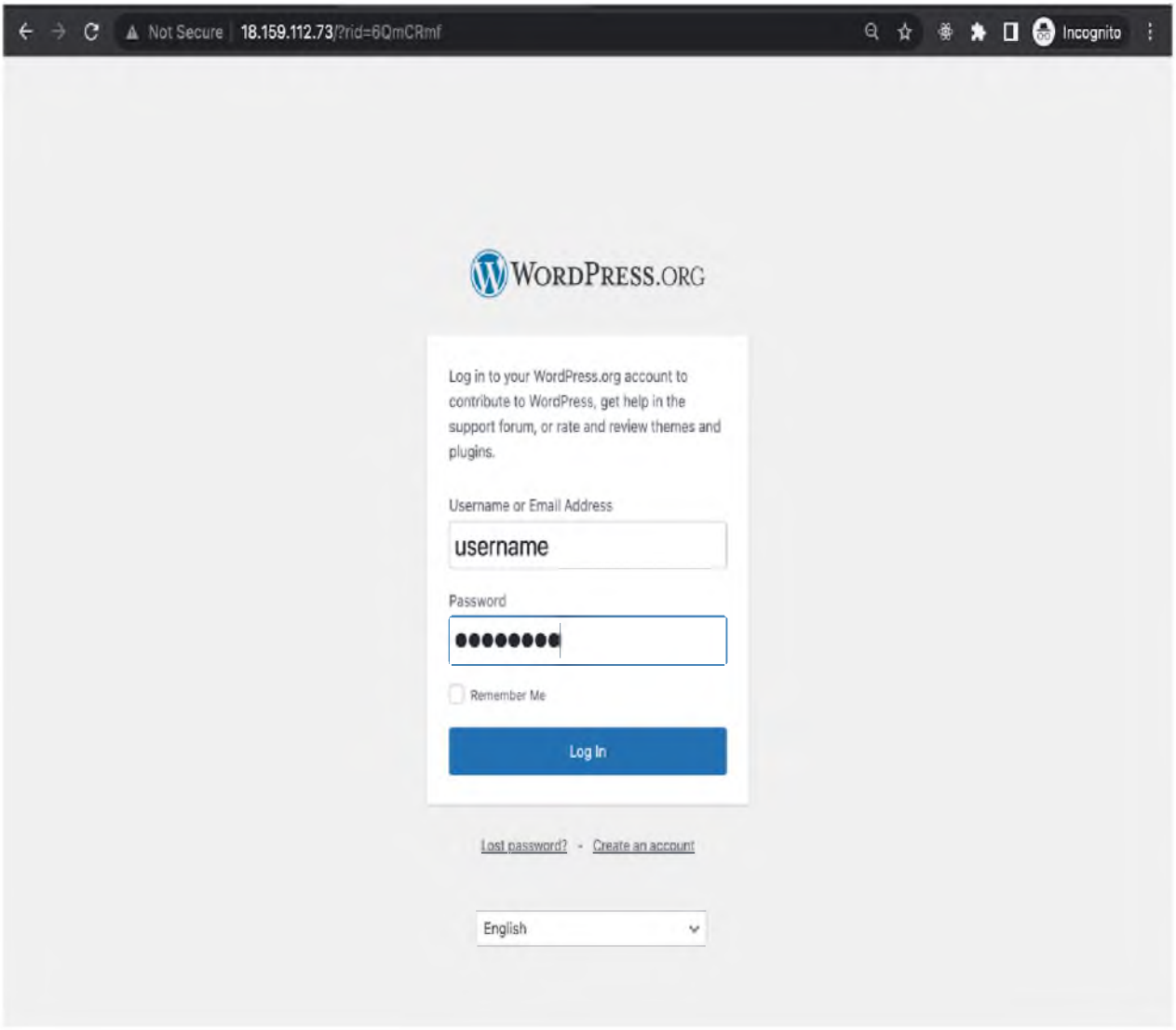

Рисунок 2.25 – Фейкова форма авторизації

Отже, маємо перший «улов»! Перевірмо, як ця інформація відображається на сторінці статистики кампаній.

Зверху на таймлайні кампанії бачимо всі події, які відбуваються (надсилання, відкриття листа, перехід за фішинговим посиланням і т. п.).

Завдяки статистиці в Gophish, можна робити перевірку певних компаній та їх співробітників, статистика показує за кожною адресою список дій, відкриття листа, перехід за посиланням, завдяки цим даним можна відслідковувати орієнтованість користувачів про фішингові атаки (рис. 2.26).

Однак Gophish використовується не лише для перевірок, а й для реальних атак та збирання інформації для особистої вигоди.

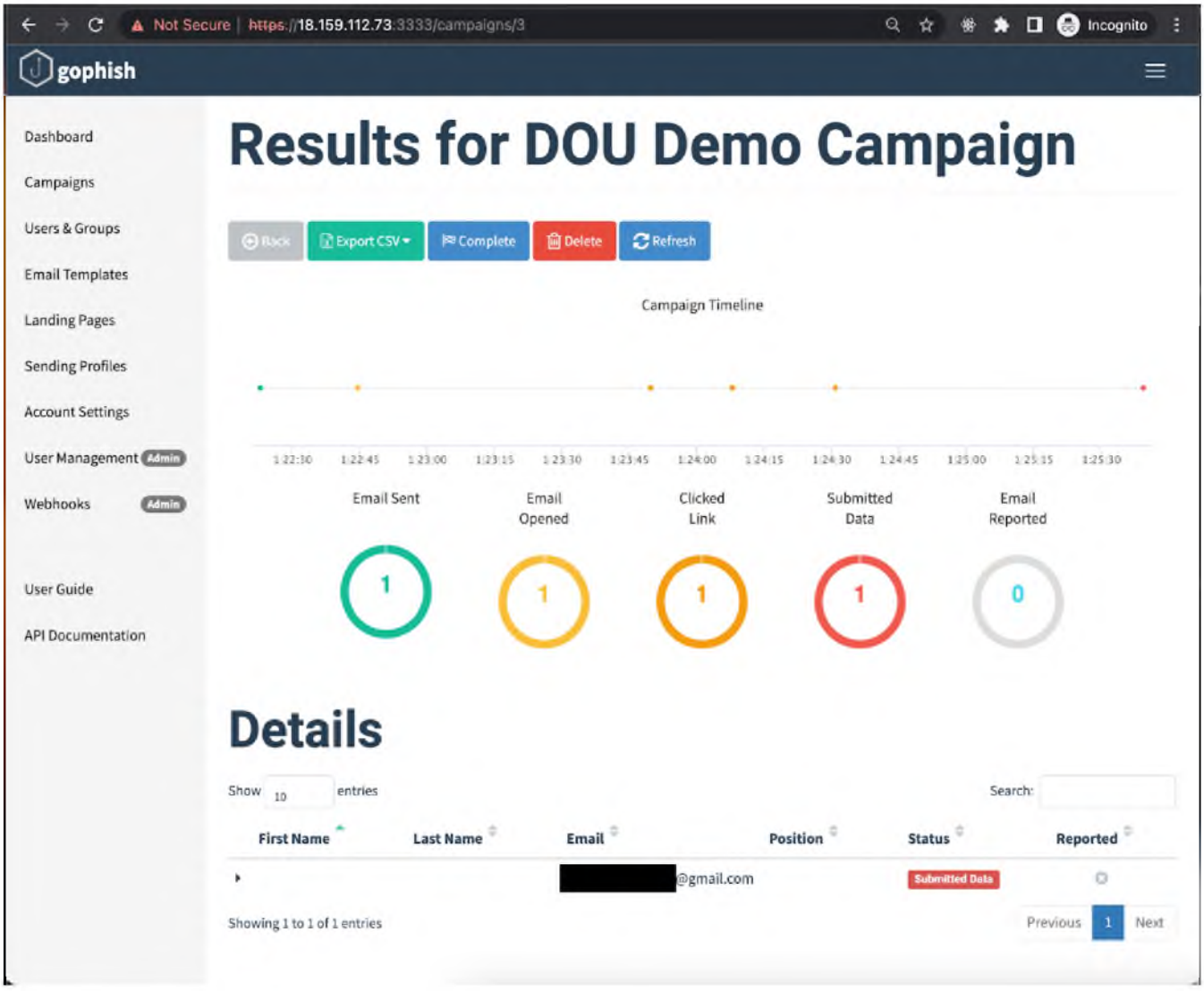

Рисунок 2.26 – Статистика за компанії в Gophish

Знизу, в секції Details, можемо переглянути інформацію за кожною ціллю. Данні, що відображаються, коли лист був доставлений, відкритий користувачем, з якого пристрою відбувався перехід і, найголовніше, дані, які «жертва» вказала у формі.

Ця статистика може бути завантажена з Gophish у виді звіту за певними категоріями, або за певними даними, наприклад можна завантажити лише список введених логінів та паролями користувачів, а можна завантажити звіт подій, хто і коли відкрив листа та які данні вводив у форму рейкової авторизації (рис 2.27).

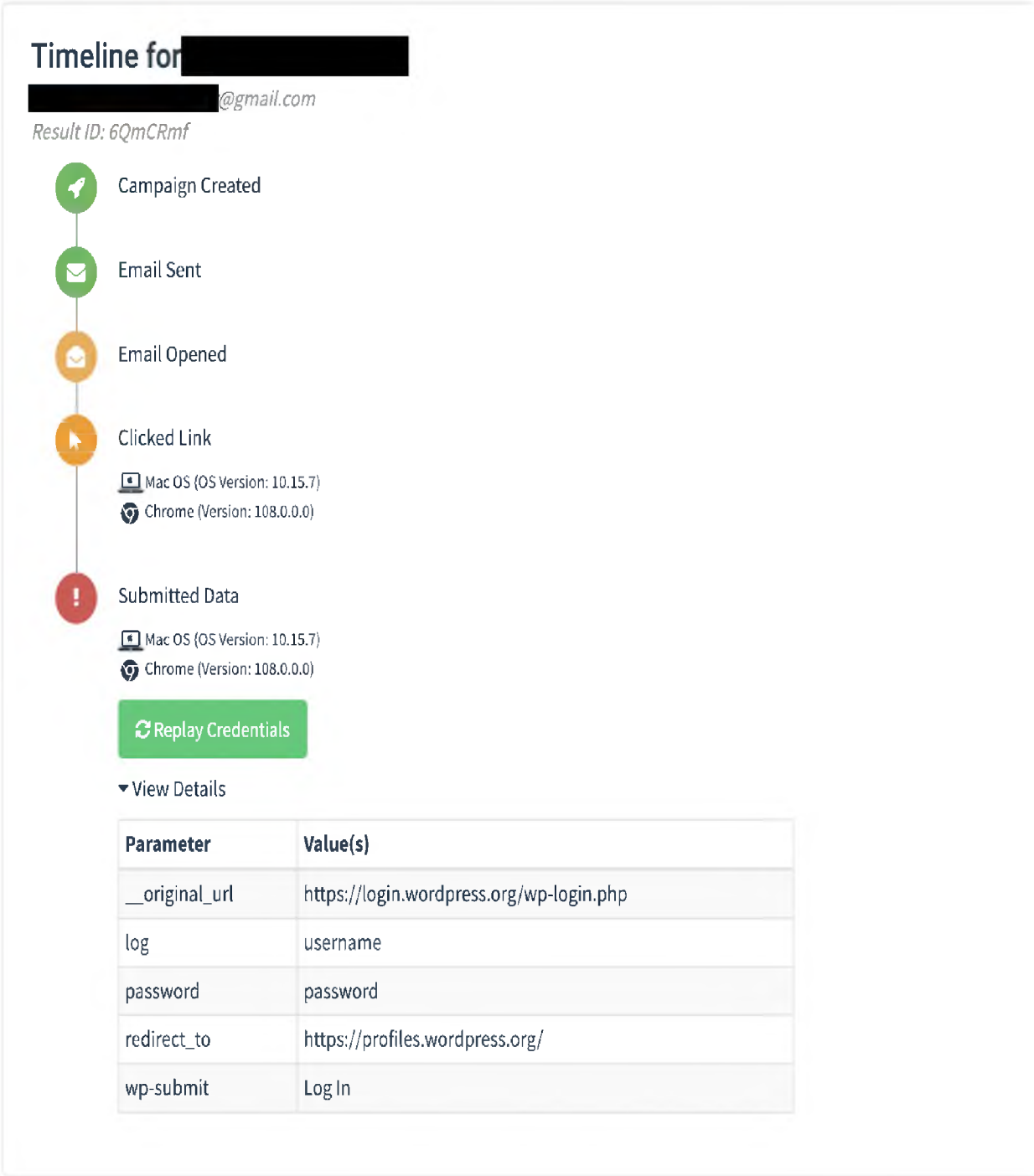

Рисунок 2.27 – Звіт за користувачем в Gophish

Підсумок

Демонстрація Gophish дала уявлення про можливості, які надає фреймворк, і розкриває етапи підготовки як до симуляцій, так і до справжніх фішингових атак. Звичайно, цей приклад може здатися дещо примітивним, тому подумаймо, які наступні кроки можна було б зробити, щоб підготувати інструмент до реального застосування.

Підібрати SMTP-сервер. У прикладі використовували SMTP сервісу розсилки, але для практичного застосування Gophish такі сервіси – навряд хороший вибір. Важливо перевірити, щоб IP SMTP сервера не були у відомих спам-списках типу Spamhaus.

Підібрати домен і прив'язати його до сервера, де буде запущений Gophish.

Налаштувати фішинговий сервер, щоб він віддавав landing pages через HTTPS. Це збільшить довіру до фішингових сторінок.

Налаштувати DNS для використання підібраного домена з нашим SMTP-сервером (SPF, DKIM, DMARC DNS-записи).

Попрацювати над deliverability вашого електронного листа. Це досить складна тема, адже на те, чи попаде ваше повідомлення в spam чи inbox, залежить дуже велика кількість факторів. Від правильності DNS-налаштувань, згаданих в попередньому пункті, до вмісту вашого листа.

Почати можна з сервісу Mail Tester. А далі, коли отримаємо максимальну оцінку, експериментувати з різними email-сервісами, адже вони можуть мати різні підходи до виявлення спаму.

Перед організацією розсилки потрібно «прогріти» SMTP-сервер і пошту, з якої буде здійснюватися розсилка. Для цього потрібно зробити кілька серій тестових розсилок зі зростальною кількістю отримувачів (наприклад: 1 день – 10, 2 – 20 отримувачів, 3 – 30 і так далі, залежно від кількості отримувачів у запланованій кампанії). Важливою є реакція отримувачів. Якщо вони відкривають лист, гортають його, переходять за посиланнями, позначають як «важливе» – все це покращує deliverability повідомлень від вашого SMTP-сервера.

2.2.2 Демонстрація фішингової атаки використовуючи метод маркетплейсів

Метод фішингу за допомогою платформ з продажу або купівлі товарів та послуг в свою чергу розширився у великих масштабах, оголошення можна знайти у будь-якій мережі(OLX, Viber, Telegram, Instagram, Facebook, Оголоша, Безплатка), інколи для такого виду шахрайства створюються сайти з рекламою продукції, щоб ще більш отримати довіри від жертв.

Спочатку необхідно вирішити на якій платформі будемо робити оголошення та визначимо правила безпеки для себе.

Використовуючи метод з пункту 2.2.1 створимо віртуальну машину на будь-який зручній платформі, під час роботи з яким необхідно буде використовувати захищене з'єднання, VPN та Proxi-сервер.

Створимо нову пошту на яку будемо реєструвати персональний кабінет на сайтах продажу товарів, після створення пошти можна одразу реєструвати особисті кабінеті, для приклада буде платформа OLX.

Вибір товару теж має велику різницю, великим попитом будуть новинки техніки, телефони та навушники, телевізори, тощо, а от старі або зламані моделі з явними дефектами навряд чи зберуть велику чергу. Необхідно написати в оголошені максимально гарний опис товару, "майже новий", "на гарантії", щоб заманити в пастку жертву.

В налаштуваннях оголошення можливі два вибори, якщо ви використовуєте телефон– використовувати дзвінки, якщо використовується як в нашому випадку віртуальна машина– використовувати лише спілкування на платформі, з часом виводити на сторонні місця спілкування.

Отже, створюємо персональну сторінку на платформі OLX, використовуючі створену пошту на віртуальну машину з функцією VPN та проксі-сервером. Обираємо товар, наприклад мобільний телефон Samsung S22 (як на рис.2.28), вказуємо низьку ціну, терміновість продажи, обираємо невелике село поряд з містом, в налаштуваннях оголошення обираємо не вказуємо номер телефону, щоб

отримувати повідомлення на платформі. Фото товара можна знайти в інтернеті, або “позичити” з інших оголошень.

Для зв’язку з жертвами створимо телеграм, оскільки для створення профіля не використовується номер телефону. Для більшої довіри поставимо фото з обличчям, вказуємо будь-яке ім’я.

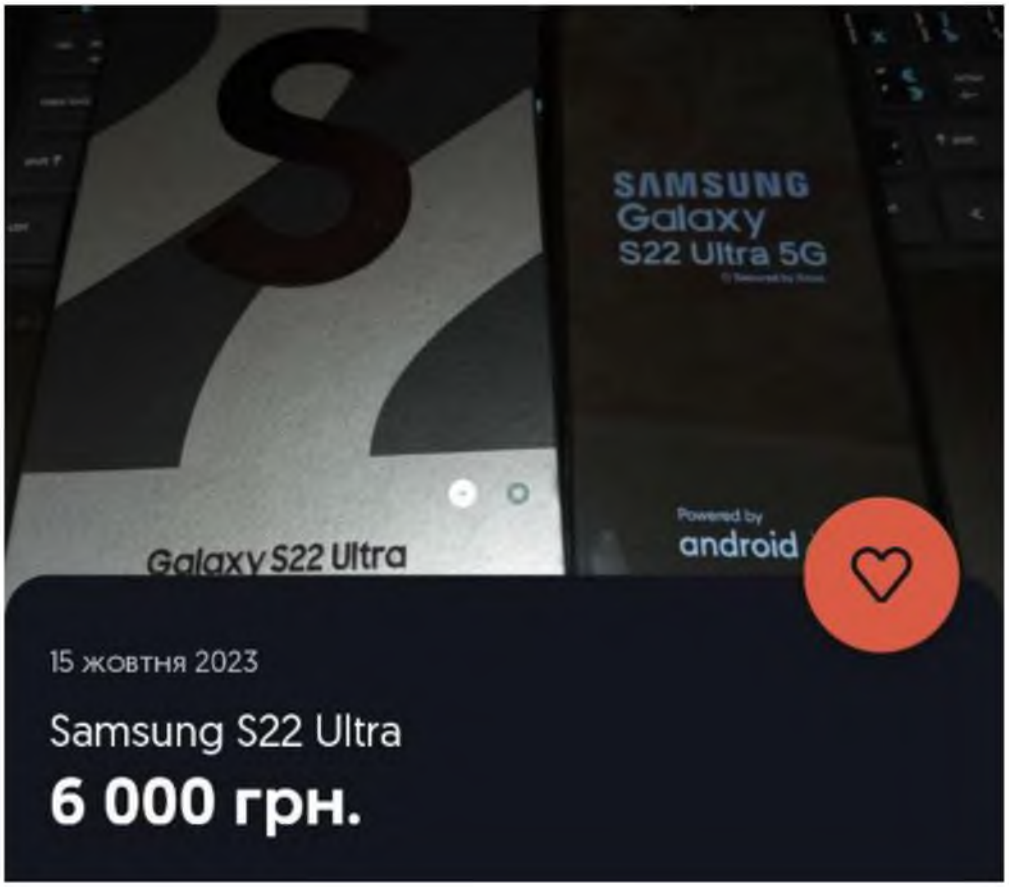

Рисунок 2.28 – Фішингове оголошення на OLX

Наступним кроком необхідно вирішити як отримувати гроші від жертви, найпростішим методом є приймати гроші на власну картку або картку подільника. Методом складніше є придбання картки з даними в так званому “Даркнеті”. Можна створити форму фейкової оплати, яка збиратиме данні карти жертв, вже потім переводити гроші на інші ресурси або одразу робити покупки на певних сервісах з метою отримати вигоду. Інший метод веде нас до криптовалюти, та методу P2P-транзакцій.

Оскільки створювати фейкову форму, така як саме представлена на рис 2.29 оплати вимагає певних навиків програмування та знань про принцип роботи онлайн транзакцій, початківці частіше за все обирають принцип PTP-транзакцій. Схема дій при цьому наступна:

– Обираємо на біржах необхідну нам валюту та шукаємо продавця, це може бути сайт-фірма з торгівлі криптовалютою або звичайний користувач;

– Створюємо ордер на необхідну нам суму, це може бути сума предоплати за наш неіснуючий товар;

– Змушуємо жертву переказати суму вказану в ордери на купівлю криптовалюти продавцеві;

– Після отримання коштів продавець відправляє на наш криптогаманець криптовалюту.

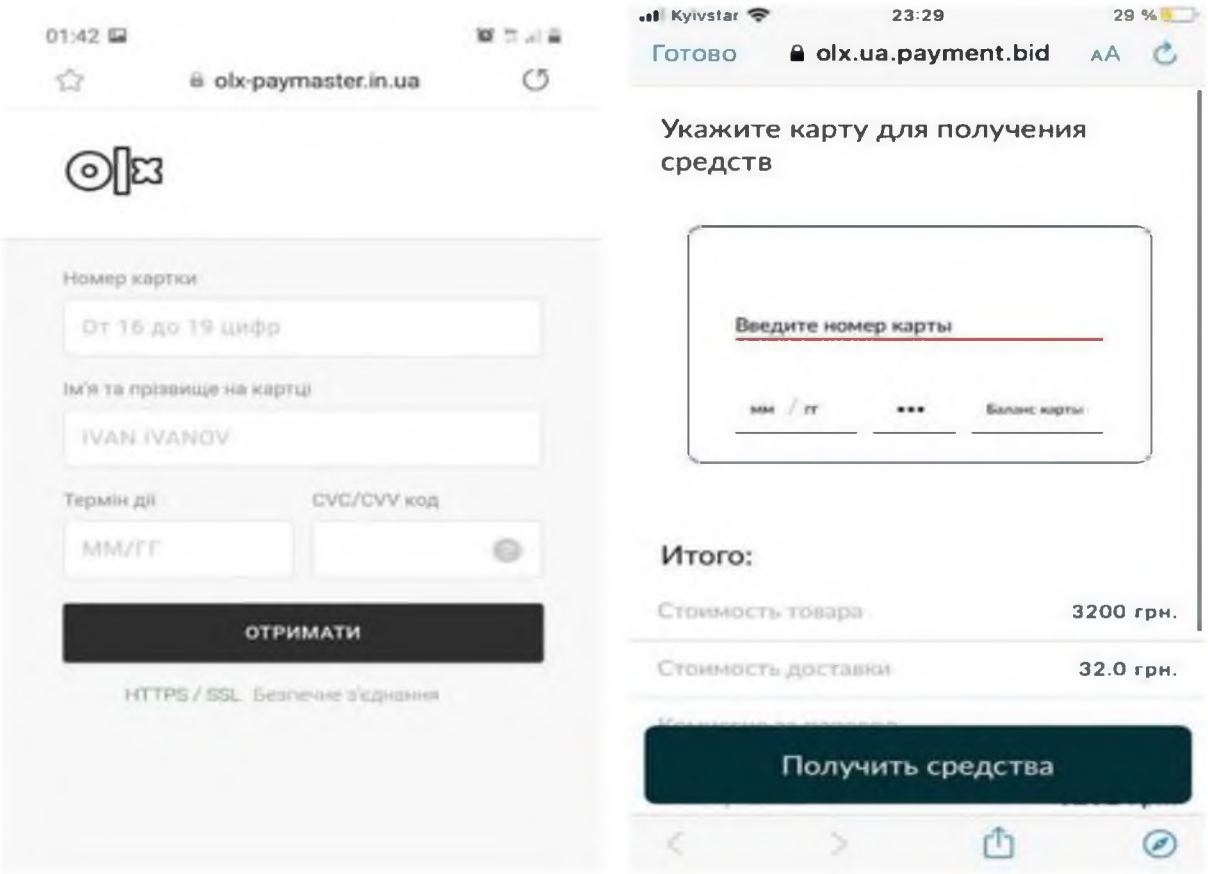

Рисунок 2.29 – Фішингова форма оплати

Найбезпечнішими методами є використання криптовалюти та фішингових форм оплати, оскільки при використанні карток банків, які можна придбати, при знятті коштів вас буде фіксувати камера на банкоматі, та буде виявлено місце, де ви знімаєте кошти.

Також можна використовувати системи переведення коштів з карти на карту, використовуючи інформацію отриману методом фішингу, але це не є надійним методом, проте краще ніж виконувати операції напряму через банк.

2.2.3 Моделювання фішингової атаки методом донатів та зборів

Збори на лікування, ЗСУ, для дітей без домівок, донати на дрони, автівки, тощо.

За останні роки повномасштабного вторгнення в Україну більшість банків зробили моделі зборів, наприклад Монобанка від Монобанку, така як на рис 2.30.

Рисунок 2.30 – Монобанка для накопичення на ремонт

Ціль таких накопичень була очевидною та мала лише добрі наміри, люди відкривали такі банки для власних цілей відкладати гроші та отримувати з них відсотки. З початком війни, відрилася функція їх поповнення від кого-завгодно, цим почали користуватися волонтері, збираючи на дрони, аптечки, тощо.

Для того, щоб люди бачили результати своїх донатів, волонтери часто роблять фото або відео звіт про придбане обладнання, виставляючи ці світлини в засоби масової інформації або соціальні мережі.

Шахраї почали користуватися даними функціями, створювати збори на "підтримку", виставляючи в соціальних мережах з нових, або вкрадених аккаунтів посилання на збір, де вказують мету підтримки ЗСУ або постраждалих від війни, користуючись матеріалами з відкритих джерел, до яких надають власні написи, номера карток чи посилання на збір.

Крадіжкою аккаунтів можна навчитися з інтернету, на цю тему у вільному доступі є різні методи до різних соціальних мереж, візьмемо за приклад Instagram. Метод прихованого файлу в текстовому файлі буде складним для реалізації шахраям без знань програмування, але при необхідності файли-крадії можна знайти у вільному доступі, цей метод буде максимально дієвим, але складним в реалізації.

Використаємо метод фішингових сайтів, але в цей раз створимо фішинговий сайт "Google Disk". Виконуємо всі інструкції з пункту 2.3.1.

Необхідно буде написати відомим блогерам, з проханням допомогти в зборі грошей для ЗСУ, поранених, тощо. Повідомивши, що вся необхідна інформація знаходиться на Google Disk, та надати наше фейкове посилання, де блогер надає нам інформацію для входу в його Google аккаунт. Після цього необхідно на вкладці авторизації натиснути кнопку "забули пароль", обрати необхідний нам спосіб відновлення через пошту, отримати посилання для відновлення пароля, після цього розпочати інформаційну атаку, а саме надсилання листів іншим знайомим з аккаунта блогера та виставляти світлини про збір грошей на нашу

Монобанку. Цей метод вимагає бути активним, оскільки через певний час аккаунт може бути заблокований.

Інший метод махінацій, це можна використовувати аккаунти з схожими назвами, та просто копіювати світлини і змінювати номер картки банку або посилання на Монобанку. На рис 2.31 нижче наведений приклад цього методу.

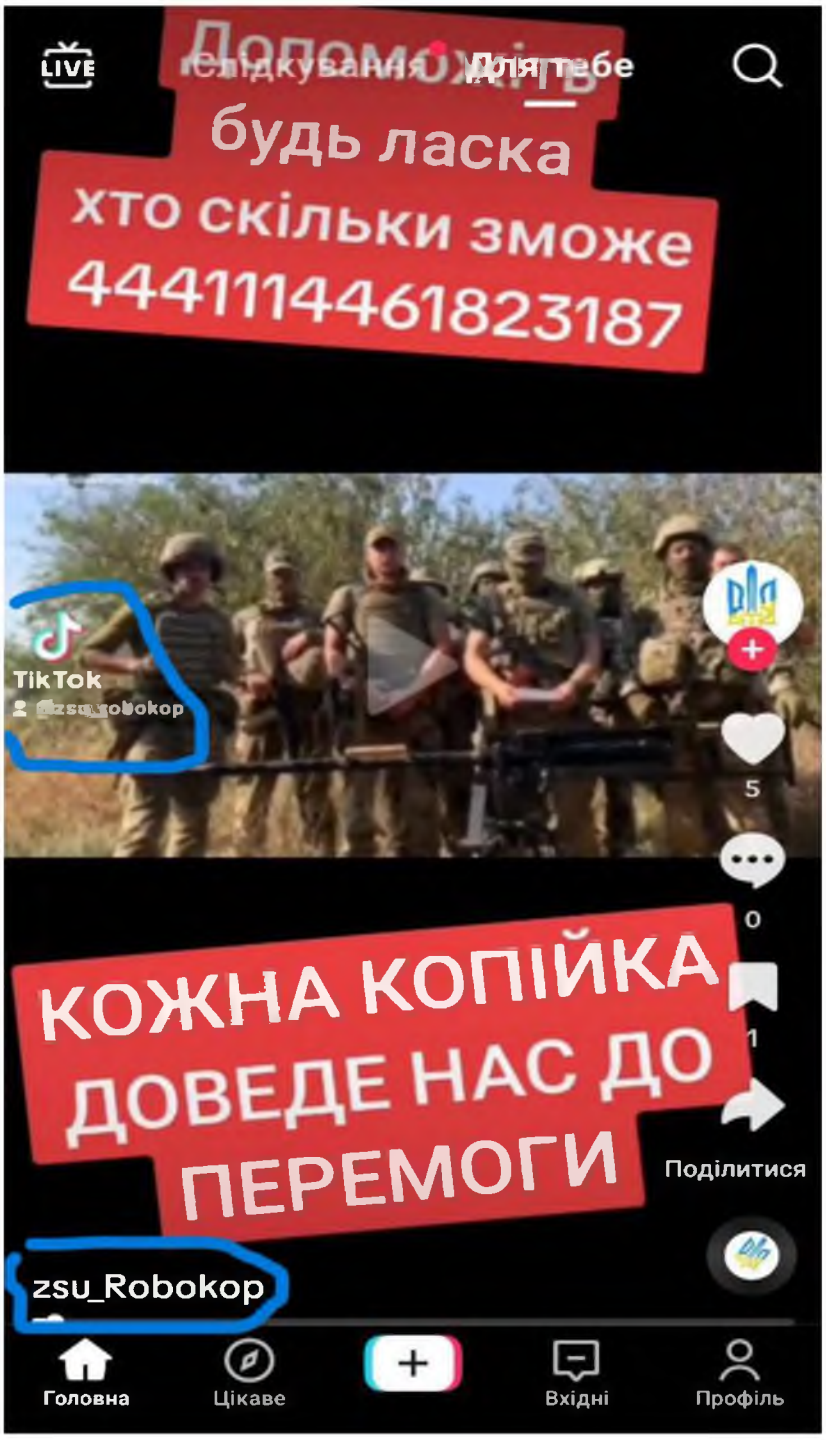

Рисунок 2.31 – Підробний аккаунт з фішинговим відео

2.3 Рекомендації щодо виявлення, запобігання, зменшення ризиків та збитків при фішингових атаках

2.3.1 Рекомендації щодо виявлення та зменшення ризиків при переході на фішингові сайти

Фішингові сайти візуально можуть мати однаковий інтерфейс, шрифт, зміст, тощо. Одним з перших методів виявлення фішингових сайтів, повинна бути власна уважність, завжди слід перевіряти посилання від малознайомих людей візуально, якщо посилання викликає сумніви, не відкривайте посилання.

Приклад оригінального та фейкового посилання:

- Оригінальне: https://www.olx.ua/
- Фейкове: https://www.olx.ukr/
- Оригінальне: https://www.privat24.ua/
- Фейкове: https://www.bankprivat24.ua/

Якщо є сумніви до посилань, необхідно самостійно знайти посилання в браузері, якому ви довіряєте, та перевіритися в безпечності наданні особистих даних. Це можна зробити за допомогою пошукової сторінки Google, де вказати необхідний нам ресурс та отримати до нього прямий доступ. При порівнянні сторінок слід дивитися на розташування елементів, шрифт, надписи, тощо, оскільки чим більше елементів знаходиться на сторінці, тим важче її ідентифікувати як фішингову. З іншого боку, якщо фішинговий сайт має візуальні елементи копії, то є велика вірогідність блокування посилання як небезпечне.

Також фішингові сайти можуть не мати SSL-сертифікатів, та майже всі сучасні браузери повідомлять вам про це (рис. 2.32), також це можна перевірити самостійно.

Рисунок 2.32– Приклад не захищеного підключення

Якщо на фішинговому сайті були введені та відправленні дані для доступу до особистого кабінету певних ресурсів, необхідно авторизуватися на цей ресурс за безпечним посиланням та змінити пароль на відмінний від старого, у разі втраченого кабінету, необхідно відновити доступ за допомогою спеціальних посилань для відновлення, якщо це не вдається, необхідно звернутися до системного адміністратора ресурсу.

Для підвищення рівня знань користувачів про фішинг, можна розповсюджувати короткі пам'ятки у виді електронних брошур, наприклад як на рисунку 2.33, брошури корисні тим, що є легкими в розробці і легкими у розповсюдженні.

Рисунок 2.33 – Приклад брошури для користувачів

При розробці брошур слід брати до уваги факт сучасних тенденцій фішингу, методів та місць їх розповсюдження. Наприклад, для маркетплейсів слід розповсюджувати брошури, які були представлені вище, для банків та методів

оплати, розробити власні, які будуть попереджувати користувачів про безпечність операцій, підвищувати рівень знань про фішинг з методами оплати, тощо.

2.3.2 Рекомендації щодо виявлення та зменшення ризиків при використанні платформ з продажу та купівлі товарів та послуг

При купівлі товарів на маркетплейсах, в першу чергу необхідно розуміти і розбиратися в товарі, який необхідно придбати, для прикладу обираємо мобільний телефон.

Щоб не потрапити у пастку фішерів, необхідно користуватися наступники правилами та методами виявлення фальшивих продавців.

При купівлі:

– При виборі товарів, порівнювати ціну і не потрапляти на “акції” з підозрілими цінами, оскільки більшість оголошень з цінами набагато нижчими за ринкові може призвести до втрати грошей або купівлі неякісного товару;

– Намагайтеся обирати продавця, який знаходиться у вашому місті, щоб робити покупку при особистій зустрічі, якщо це неможливо, оглядайте посилку на пошті в присутності співробітника пошти і якщо товар вас розчарував, або взагалі отримали не те, на що розраховували, відмовляйтесь від посилки. Посилки які вказано “не оглядати” швидше за все будуть фішинговими, оскільки стандартні протоколи пошти не передбачають таку примітку.

– Використовуйте лише перевірені магазини та способи оплати, не переходьте за посиланнями які надходять від продавця, якщо це можливо, використовуйте захищенні методи доставки, наприклад OLX-доставка, у самому застосунку.

– Не використовуйте часткову передплату, бронювання, інші варіанти, де намагаються отримати гроші завчасно.

– У разі потрапляння до зловмисників, фіксуйте відкриття коробки, стан товару, документи на отримання, тощо. Надайте інформації правоохоронним

органам, зверніться до підтримки пошти та платформи, на якій були придбані товари.

– Перевіряти продавця на платформах, коли був створений особистий кабінет, товари що він продає, за номером телефону в відкритих джерелах.

При оплаті товару можна додати спливаючу пам'ятку, яка буде сигналом того, що сайт оплати є безпечним, навіть якщо вона буде на фішингових сайтах, то допоможе суцільно знизити ризики потрапляння до фішингових форм оплати, приклад наведено на рисунку 2.34, для більш точного формулювання слід використовувати маркери самого методу оплати, наприклад Моно чи Приват24 з інструкцією як відрізнити оригінал.

Рисунок 2.34 – Приклад брошури-маркера для користувачів сайтів переказу коштів

В разі продажу товару:

– Ведіть переписку на платформі, не переходячи до спілкування в сторонніх месенджерах.

– Товар необхідно надсилати лише перевіреними поштовими представниками, при відправці вказувати оголошену вартість та не відмовлятися

від страхування посилок. Ні в якому разі не віддавати посилку стороннім особам ”брат забере”, за можливості фіксувати відправлення.

– При поверненні товару перевіряти його на почті, оскількі інколи бувають випадки кражі товару.

Дотримуючись цих правил, можна зменшити ризики потрапляння в пастку до шахраїв. Також на більшості платформах, або у вільному доступі в інтернеті, можна знайти рекомендації стосовно користування певними платформами, їх правила та застереження від шахраїв, але на цих сторінках не робиться великий акцент. Оскільки реальні дані по середньому рівні користування персональним комп’ютером та інтернетом дуже відрізняються, більшість обмежень, застережень та посібників з користування ресурсами знаходяться в глибині самих ресурсів та не прикладаються для початку користуванням сервісом.

2.3.3 Рекомендації щодо виявлення та зменшення ризиків при благодійних внесках до зборів, донатів, тощо

Одна з повсякденних тем на сьогодення, збори для військових на автівки, дрони, медицину, збір коштів на поранених, тощо. Визначення фейкових зборів для звичайного користувача інтернетом є певною перешкодою, оскільки не всі користувачі володіють гарними пошуковими навичками.

Для того, щоб не стати жертвою фейкових зборів, не перевести добровільно власні гроші шахраям, необхідно мати добру дедукцію, методи сприйняття та аналізу інформації.

Основні пункти для зменшення ризиків, при благодійності в інтернеті:

– Знаходити фонди, посилання на донати та збори з популярних або спеціальних джерел.

– Не переходити і не користуватися посиланнями від мало відомих або ненадійних джерел.

– При використанні джерел з відомостями про донати, порівнюйте номера банківських карт, звіти з закупівель, історію витрат. Це необхідно для того, щоб відстежити зміну банківських рахунків і розуміння про дійсність збору.

– При наявності водяних знаків, можливо знайти першо-джерело та порівняти платіжну інформацію.

– Робити перекази в мобільному банкінгу, не передаючи данні від банківських карт у невідомих формах оплати, тощо. Оскільки більшість сучасних платформ мають власні форми оплати, слід користуватися ними.

– Довіряти відкритим зборам, які демонструють результати зборів, чеки про закупівлю, відео-фото фіксацію передачі дронів, автівок, тощо. Ці збори є максимально прозорими і кожна людина може відслідковувати, на що були використані гроші.

– Не переводити гроші, при переписці з людьми, від яких приходить повідомлення з проханням, оскільки це може бути втрачений аккаунт з якого роблять СПАМ-розсилку.

2.4 Висновки

У другому розділі кваліфікаційної роботи було проведено дослідження про методики впливу на жертву соціальної інженерії, а також реальні експлойти, які застосовуються у великій більшості фішингових атак. Продемонстровані основні методи фішингу, на прикладах фішингового сайту підробки з використанням віртуальної машини та додатку Gophish, фейкового оголошення на торгівельних площадках та при благодійних онлайн зборах і донатах. Визначені моделі поведінки та методи крадіжки особистих даних користувачів та розроблені правила користування застосунками, щоб зменшити ризики, та вчасно виявити небезпеки у разі потрапляння до пасток фішерів.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Обґрунтування витрат на впровадження рекомендацій для користувачів

Метою розділу є визначення доцільності розробки та поширення універсальних та спеціалізованих правил поводження, користуванням інтернетом, певними ресурсами, які можуть бути використанні в злочинній діяльності з метою отримання нелегального прибутку.

Головною метою кваліфікаційної роботи полягаю підвищення рівня знань про користування і небезпеку в інтернеті, зменшення рівня кібершахрайств, зменшення рівня запитів до поліції та кіберполіції.

Для підвищення рівня обізнаності в користуванні інтернетом і небезпекам, пов’язаним з фішингом, необхідно розробити правила користування ресурсами, на яких великий попит у фішерів, підвищити рекламу таких правил для більшої зацікавленості та вивчені користувачами.

Збільшення кількості продвинутих користувачів, які будуть самостійно викривати фішерів, зменшить кількісне навантаження на правоохоронну, судочинну, адміністраторів платформ, страхові, державну, тощо.

В Економічному розділі розрахуємо капітальних витрат на придбання і налагодження складових системи для підвищення обізнаності користувачів інтернету та витрат, що пов’язані з виготовленням апаратури та програмного забезпечення; річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування; річного економічного ефекту; показників економічної ефективності розробки та впровадження запропонованих рішень.[6]

3.2 Розрахунки витрат

Нормування праці в процесі створення рекомендацій істотно ускладнено через творчій характер праці програмістів та фахівців з питань кібербезпеки. Проте трудомісткість розробки і опрацювання ПЗ може бути розрахована на основі системи моделей з певною точністю оцінки. Трудомісткість створення

рекомендацій визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації.

$$t = t_{тз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{б}\text{ , годин} \quad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку ПЗ;

$t_{в}$ – тривалість вивчення ТЗ, літературних джерел за темою тощо;

$t_{а}$ – тривалість розробки рекомендацій і матеріалів;

$t_{пр}$ – тривалість програмування платформ для оприлюднення рекомендацій;

$t_{опр}$ – тривалість опрацювання рекомендацій на платформах і їх поширення;

$t_{б}$ – тривалість підготовки технічної документації для рекомендацій.

Підрахуємо трудомісткість: $t_{тз}$ = 14 годин;

$t_{в}$ = 22 години;

$t_{а}$ = 8 годин;

$t_{пр}$ = 8 годин;

$t_{опр}$ = 2 години;

$t_{б}$ = 4 години.

Використовуючи формулу (3.1) обчислюємо трудомісткість створення ПЗ:

$$t = 14 + 22 + 8 + 8 + 2 + 4 = 58 \text{ годин.}$$

Витрати на створення рекомендацій Кпз складаються з витрат на заробітну плату виконавця рекомендацій, їх публікування і поширення Ззп і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК Змч :

$$К_{пз} = З_{зп} + З_{мч}\text{, тис. грн} \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{зп} = t\ x\ З_{пр}\text{, грн} \quad (3.3)$$

де t – загальна тривалість створення рекомендацій, годин;

$з_{пр}$ – середньогодинна заробітна плата спеціаліста з питань кібербезпеки з нарахуваннями, грн/годину. Використовуючи формулу (3.3) обчислюємо заробітну плату виконавця:

$$З_{зп} = 58 \, x \, 175 = 10150 \text{ , грн.}$$

Вартість машинного часу для налагодження рекомендацій на платформі визначається за формулою:

$$З_{мч} = t_{опр} \, x \, С_{мч} + t_{б}, \text{ грн,} \quad (3.4)$$

де $t_{опр}$ – трудомісткість налагодження рекомендацій на платформі, годин;

$t_б$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = P \, x \, t_{нал} \, x \, С_е + (Ф_{зал} \, x \, Н_а) / F_р + (К_{лпз} \, x \, Н_{апз}) / F_р \text{ , грн,} \quad (3.5)$$

де Р – встановлена потужність ПК, кВт;

$t_{нал}$ – кількість ПК;

$С_е$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920).

Використовуючи формулу (3.5) обчислюємо вартість 1 години машинного часу ПК:

$$С_{мч} = 0{,}3 \, x \, 2 \, x \, 2{,}64 + (6000 \, x \, 0{,}5)/1920 + (5000 \, x \, 0{,}25)/1920 = 4{,}45 \text{ грн.}$$

Використовуючи формулу (3.4) обчислюємо вартість машинного часу для налагодження рекомендацій на ПК:

$$З_{мч} = 2\,x\,4{,}45 + 4 = 12{,}9 \text{ грн.}$$

Використовуючи формулу (3.2) обчислюємо витрати на створення програмного продукту:

$$К_{пз} = 10150 + 12{,}9 = 10162{,}9 \text{ грн.}$$

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи підвищення рівня обізнаності користувачів з питань фішингу складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}, \text{ грн.} \quad (3.6)$$

де $К_{пр}$ – вартість розробки рекомендацій для користувачів та залучення для цього зовнішніх консультантів, тис. грн (3100 грн вартість розробки проекту та 2900 грн вартість послуг залучених зовнішніх консультантів);

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн (Windows 10 Pro – 3600 грн на рік, антивірус 360 Total Security – 1200 грн ліцензія на рік, Visual Studio та Microsoft Office – 1400 грн);

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн (у разі виникнення потреби для певних платформ, де не розроблена можливість інформування користувачів);

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн (твердотільний диск SSD 128 GB – 1500 грн);

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн (послуги навчання персоналу – 1000 грн);

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн (послуги спеціаліста з налаштування реклами і роботи з контентом – 1200 грн).

Використовуючи формулу (3.6) обчислюємо витрати на капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки:

$$K = 6000 + 6200 + 0 + 1500 + 1000 + 1200 = 15900 \text{ грн.}$$

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

Отже, річні поточні (експлуатаційні) витрати на функціонування системи підвищення обізнаності користувачів складають:

$$C = C_в + C_к + C_{ак} + C_{ам}, \text{ тис. грн.} \quad (3.7)$$

де $C_в$ – витрати на Upgrade-відновлення й модернізацію системи (20% від капітальних витрат);

$C_{ак}$ – витрати, викликані активністю користувачів системи підвищення обізнаності користувачів (10% від капітальних витрат);

$C_{ам}$ – амортизаційні витрати системи, які є фіксованими в залежності від очікуваних навантажень на систему, ціну тарифу інтернет послуг, електроенергії та обслуговуючого персоналу компанії (15% від капітальних витрат);

$C_к$ – керування системою підвищення обізнаності користувачів, визначається за формулою:

$$C_к = C_{ел} + C_{тос} \quad (3.8)$$

де $C_{ел}$ – Вартість електроенергії, що споживається апаратурою системою підвищення обізнаності користувачів протягом року;

$C_{тос}$ – Витрати на технічне й організаційне адміністрування та сервіс системи підвищення обізнаності користувачів;

$C_{ел}$ визначається за формулою:

$$C_{ел} = P \, x \, F_р p \, x \, C_е, \text{ грн} \quad (3.9)$$

Використовуючи формулу (3.9) обчислюємо вартість електроенергії, що споживається апаратурою системи підвищення обізнаності користувачів протягом року:

$$C_{ел} = 0{,}3\ x\ 1920\ x\ 2{,}64 = 1520{,}64 \text{ грн.}$$

Використовуючи формулу (3.8) обчислюємо витрати на керування системою підвищення обізнаності користувачів $C_к$:

$$C_к = 1520{,}64 + (15900 \text{ x } 0.02) = 1838{,}64 \text{ грн.}$$

Використовуючи формулу (3.7) обчислюємо річні поточні (експлуатаційні) витрати на функціонування системи підвищення обізнаності користувачів:

$$C = 0{,}2\ x\ 15900 + 1838{,}64 + 0{,}10\ x\ 15900 + 0{,}15\ x\ 15900 = 8993{,}64 \text{ грн}$$

де $C_в$ – витрати на Upgrade-відновлення й модернізацію системи підвищення обізнаності користувачів (20% від капітальних витрат);

$C_{ак}$ – витрати, викликані активністю користувачів системи підвищення обізнаності користувачів (10% від капітальних витрат);

$C_к$ – керування системою підвищення обізнаності користувачів.

Тепер розглянемо можливі втрати через відсутність розвитку інформаційної безпеки на платформах та у користувачів цих платформ, паралельно з розвитком кібершахраїства. Витрати у разі відбуття інциденту кібершахрайства необхідно вимірювати з обох сторін, сторона держави і приватна сторона впродовж року:

$$П_{ви} = \sum З_o + F\ x\ t_в = 2211\ x\ 324 + 95\ x\ 3168 = 1017324 \text{ грн}$$

Середня вартість попадання на фішингових приманках складає приблизно 2211 грн, кількість заяв, що реєструються впродовж року одним співробітником складає 324 справ.

Де середньогодинна заробітня плата співробітника полціції – 95 грн, а час роботи на рік $t_в$ = 3168 годин.

Загальний ефект від впровадження системи підвищення інформаційної грамотності населення з питань кібербезпеки і користуванням інтернетом і спеціалізованих платформ з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C \quad (3.10)$$

Де В – загальний збиток від вдалої атаки на персональні данні, тис. грн (врахуємо 3168 годин на рік);

R – очікувана кількість вдалих атак, після яких було складено протокол, частки одиниці;

С – щорічні витрати на експлуатацію системи підвищення інформаційної грамотності суспільства і підвищення знань з користування платформами з ризиками фішингу (як вже підрахували 8993,64 грн).

Підрахуємо загальний ефект від впровадження системи інформаційної безпеки:

$$E = (95 \; x \; 3168) \; x \; 0{,}15 - 8993{,}64 = 36150{,}36 \text{ грн.}$$

Розрахуємо також оцінку економічної ефективності системи підвищення інформаційної грамотності населення з питань кібербезпеки і користуванням інтернетом і спеціалізованих платформ. Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи. Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від фішингових атак та їх варіацій, а отже:

$$ROSI = E \; / \; K \quad (3.11)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки, тис. грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, (приблизно 16000 тис. грн)

Підрахуємо коефіцієнт

$$ROSI = 36150{,}36 / 16000 = 2{,}25$$

Можемо зробити висновок, що коефіцієнт повернення інвестицій вказує на перспективність інвестицій даного проекту.

3.3 Висновки

У розділі були підраховані суми капітальних (фіксованих) витрат на проектування та впровадження проектного варіанта системи підвищення інформаційної грамотності населення з питань кібербезпеки і користуванням інтернетом і спеціалізованих платформ та річних поточних (експлуатаційних) витрат на функціонування системи, які склали 15900 та 8993,64 грн відповідно, коефіцієнт ROSI становить 2,25. Розробку і впровадження рекомендацій для користувачів можна назвати доцільним, адже спираючись на статистичні дані збитків через фішингові атаки, витрачені кошти на створення системи видачі рекомендацій дозволять суттєво зменшити поточні витрати організацій та держави на ліквідацію наслідків порушень ІБ.

ВИСНОВКИ

У кваліфікаційній роботі розкрили актуальність теми кібершахрайства в Україні, а саме фішингу та йому подібних методів. Визначили мету фішингу та його історію розвитку. Розкрили проблему малої обізнаності користувачів, щодо фішингу та кібербезпеки при користуванні інтернетом, а саме маркетплейсів, відсутністю знань про фішингові сайти, можливість омани при зборах та донатах, тощо. Розкрили питання про підвищення навичок та знань у користувачів, які зіштовхуються з певними моделями фішингу під час роботи з інтернетом та певними платформами.

Під час аналізу статистики визначили вразливі групи користувачів, основні дії при зіткненні з фішингом в інтернеті, реакції та дії користувачів, які стали жертвами фішингу. Проаналізували витрати держави, страхових компаній, банків та користувачів від фішингу у порівнянні за декалька років, дослідили важливість розвитку знань у користувачів інтернету знань про особисту безпеку і безпеку персональної і банківської інформації.

В спеціальному розділі визначили, яку роль грає соціальна інженерія під час впливу на жертву та розглянули основні методи впливу та методи протидії, яку може застосовувати жертва, щоб не піддатися впливу.

Розглянули методи створення фішингової інтернет сторінки на стенді, методи збору персональної інформації жертви та використання її в особистих інтересах. Продемонстрували роботу фішингової сторінки, фішингової об'яви на маркетплейсі, методи впливу на жертву з використанням соціальної інженерії, метод фішингу за допомогою зборів і донатів.

Розробили рекомендації для підвищення рівня досвідченості користувачів в сфері кібербезпеки та протидії фішинговим атакам. Запропонували інтерактивні методи підвищення рівня знань з фішингу шляхом розповсюдження буклетів при початку користування ресурсом.

В економічному розділі кваліфікаційної роботи визначили фінансову актуальність теми для держави, держслужбовців які працюють в сфері

забезпечення кібербезпеки в державному правовому полі. Розрахували капітальних витрат на придбання і налагодження складових системи для підвищення обізнаності користувачів інтернету та витрат, що пов’язані з виготовленням апаратури та програмного забезпечення; річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування; річного економічного ефекту; показників економічної ефективності розробки та впровадження запропонованих рішень. Коефіцієнт повернення інвестицій ROSI показав гарний результат, тому проект можна вважати економічно доцільним.

ПЕРЕЛІК ПОСИЛАНЬ

1. Комп'ютерне шахрайство [Електронний ресурс] // Вікіпедія – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B5_%D1%88%D0%B0%D1%85%D1%80%D0%B0%D0%B9%D1%81%D1%82%D0%B2%D0%BE.
2. Фішинг [Електронний ресурс] // Вікіпедія – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%A4%D1%96%D1%88%D0%B8%D0%BD%D0%B3.
3. Думчиков С. А. СТАТИСТИКА ФІШИНГОВИХ ІНЦИДЕНТІВ В УКРАЇНІ ЗА 2021 РІК [Електронний ресурс] / С. А. Думчиков, В. В. Лукічов. – 2022. – Режим доступу до ресурсу: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/34523/91970.pdf?sequence=2&isAllowed=y.
4. Фішинг — що це таке, суть, визначення, види та приклади фішингу. [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://termin.in.ua/fishynh/.
5. Кіберзлочинність: виклики часу [Електронний ресурс]. - 2023- Режим доступу до ресурсу: https://law.chnu.edu.ua/kiberzlochynnist-vyklyky-chasu/
6. Інформаційна та кібербезпека: чому це важливо для бізнесу [Електронний ресурс]. - 2023- Режим доступу до ресурсу: https://www.softline.kiev.ua/news/informatsiina-ta-kiberbezpeka-chomu-tse-vazhlyvo-dlia-biznesu.html
7. ISO 27001 [Електронний ресурс] // ISO. – 2022. – Режим доступу до ресурсу: https://www.iso.org/ru/standard/27001.

8. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: Д.П. Пілова – Дніпро: Національний технічний університет «Дніпровська політехніка», 2017. – 17 с.
9. Кваліфікаційна робота магістра. Методичні рекомендації до виконання для студентів спеціальності 125 «Кібербезпека» (освітньо-професійна програма «Кібербезпека») / Упоряд.: О.Ю.Гусєв, В.І.Корнієнко, В.І.Магро, Д.С. Тимофєєв; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Д.: НТУ «ДП», 2022. – 34 с.
10. NIST SP 800-501 [Електронний ресурс]. - 2003. -Режим доступу до ресурсу:https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf.
11. НД ТЗІ 1.1-003-99 - Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 28.04.1999]- К. : ДСТСЗІ СБУ, 2005. - No22 - (Нормативний документ системи технічного захисту інформації).
12. HM Government, "Технічний звіт" 2015.
13. Information and S. Survey, «Боротьба за усунення розриву», 2012.
14. Офіційний сайт ISACA. COBIT [Електроний ресурс]. – Режим доступу https://www.isaca.org/resources/cobit/
15. Information technology. Security techniques. Information management. Measurement: ISO/IEC 27004:2016 [Електронний ресурс]. Режим доступу: https://www.iso.org/standard/64120.html
16. Як захистити себе в інтернеті [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://ms.detector.media/trendi/post/26505/2021-01-28-yak-zakhystyty-svoi-personalni-dani-v-interneti-vidpovidayut-eksperty-rady-ievropy/.
17. Види фішингу в Українському інтернеті [Електронний ресурс] // UA News. – 2022. – Режим доступу до ресурсу:

https://ua.news/ua/technologies/yaki-vydy-fishyngu-vykorystovuyut-shahrayi-na-ukrayinskyh-marketplejsah.

18. Як розпізнати фішинговий сайт [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://web-promo.ua/blog/chek-list-dlya-proverki-sajta-kak-raspoznat-fishingovyj-sajt/.
19. Фішинг в благодійності [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://dev.ua/news/shakhrai-blahodiinoi-dopomohy.
20. Фішинг в тік тоці [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://gridinsoft.ua/blogs/populyarni-shemy-shahrajstva-u-tiktok/.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	20	
6	А4	2 Розділ	40	
7	А4	3 Розділ	8	
8	А4	Висновки	2	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 95 б. («Відмінно»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу магістра на тему:

Методи виявлення та протидії фішингу в соціальних мережах та месенджерах

студента групи 125м-22-1

Хуторного Олександра Сергійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 86 сторінках та містить 38 рисунків, 2 таблиць, 20 джерел та 4 додатка.

У кваліфікаційній роботі розглядається проблематика та актуальність кібербезпеки на сьогодення. Основні теми та тезиси для розкриття теми фішингу.

Визначено актуальність питання підвищення рівня знань користувачів з наведенням статистики збитків держави та банківських установ. Визначено мету фішингових атак, їх види, механізм з урахування соціальної інженерії. Наведено реальний приклад фішингу та стандартні рекомендації.

Розкрито поведінку порушника, його тактику та основні прийоми під час активної фази фішингу, розглянуто сучасні моделі фішингу та їх реалізацію на стенді зі створенням фішингового сайта з отриманням даних від користувачів, створено універсальну пам’ятку для користувачів про безпеку в інтернеті для певних платформ розповсюждення.

Практичне значення роботи полягає у підвищенні знань про шахрайство в інтернеті з метою зменшення кількості кіберзлочинів.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник спец. частини

ст. викл. каф. БІТ Вадим МЄШКОВ